CA Process Automation

Handbuch für Inhaltsadministratoren

Version 04.2.00



CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA Catalyst für CA Service Desk Manager (CA Catalyst-Connector für CA SDM)
- CA Client Automation (früher CA IT Client Manager)
- CA Configuration Automation (früher CA Cohesion® Application Configuration Manager)
- CA Configuration Management Database (CA CMDB)
- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA Infrastructure Insight (früher im Paket: CA Spectrum IM und CA NetQoS Reporter Analysator kombiniert)
- CA NSM
- CA Process Automation (früher CA IT Process Automation Manager)
- CA Service Catalog
- CA Service Desk Manager (CA SDM)
- CA Service Operations Insight (CA SOI) (früher CA Spectrum® Service Assurance)
- CA SiteMinder®
- CA Workload Automation AE

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Änderungen in der Dokumentation

Die folgenden Dokumentationsaktualisierungen sind seit der letzten Ausgabe dieser Dokumentation vorgenommen worden:

- Hinzufügen neuer Anwender zu CA Process Automation (siehe Seite 60): Dieses vorhandene Thema wurde mit Verweisen auf das neue *Benutzeroberflächen-Referenzhandbuch*, das Feldbeschreibungen enthält, aktualisiert.
- Beispiel: Ein Einzelanwender in zwei referenzierten Active Directory-Verzeichnissen (siehe Seite 66): Dieses neue Thema enthält ein Beispiel für CA Process Automation-Anwender, auf die CA EEM-Verweise aus mehreren Microsoft Active Directory-Verzeichnissen vorliegen, in denen derselbe Anwender in mehr als einem AD-Verzeichnis definiert ist.
- Konfigurieren von CA EEM-Sicherheitseinstellungen für die Domäne (siehe Seite 150): Dieses vorhandene Thema wurde mit einer Beschreibung von "Standardmäßige Active Directory-Domäne" aktualisiert. Dabei handelt es sich um ein Feld, das nur anwendbar ist, wenn CA EEM für die Verwendung mehrerer Microsoft Active Directory-Domänen konfiguriert ist.
- Konfigurieren von Domäneneigenschaften (siehe Seite 156): Dieses vorhandene Thema wurde aktualisiert, um Beschreibungen neuer Felder für Hostgruppenkonfiguration und Bereinigung von Berichtsdaten einzuschließen. Weitere Themen, die auf ähnliche Weise für Hostgruppenkonfiguration aktualisiert wurden:
  - Konfigurieren von Umgebungseigenschaften (siehe Seite 169)
  - Konfigurieren der Eigenschaften eines Koordinationsrechner-Kontaktpunkts (siehe Seite 186)
  - Konfigurieren der Hosteigenschaften des Koordinationsrechners (siehe Seite 193)
  - Sicherstellen einer effizienten Verarbeitung von Hostgruppen-Referenzen (siehe Seite 279)
- Interaktives Installieren eines Agenten (siehe Seite 215): Dieses vorhandene Thema wurde aktualisiert, um ein neues Kontrollkästchen zu dokumentieren, über das angegeben wird, ob der Agent vereinfachte Kommunikation (NGINX oder F5) oder veraltete Kommunikation (Apache oder F5) verwenden soll. Es ist auch festgehalten, dass Windows sowohl JRE7 als auch JRE6 unterstützt. Weitere Themen, die mit Informationen zu neuen Kommunikationsmethoden aktualisiert wurden:
  - Konfigurieren von Agenteneigenschaften (siehe Seite 220)
  - Informationen zur Agent-Kommunikation (siehe Seite 232)

- Konfigurieren von Agenten zur Verwendung von vereinfachter Kommunikation (siehe Seite 233)
- Konfigurieren von Agenten zur Verwendung von veralteter Kommunikation (siehe Seite 233)

- Szenario: Einrichten von Kontaktpunkten für Design und Produktion (siehe Seite 237): Dieses neue Szenario kombiniert vorhandene Informationen, um zu veranschaulichen, wie sich die Konfigurationsoptionen, die in einer Produktionsumgebung verwendet werden, von jenen in einer Designumgebung unterscheiden.
- Fälle, in denen das Verwenden von Hostgruppen-Referenzen vermieden werden soll (siehe Seite 280): Dieses neues Thema behandelt die Auswirkungen der Angabe einer IP-Adresse als Operatorziel für das Verteilen eines Prozesses an eine Umgebung oder Domäne, in der das Ziel ein abweichender Host ist. Prozesse, die als vordefinierter Inhalt exportiert und importiert werden, können nicht geändert werden.
- Konfigurieren der Operatorkategorien (siehe Seite 289): Alle Themen in diesem vorhandenen Abschnitt wurden überarbeitet, um Feldbeschreibungen zu entfernen, die nun im *Benutzeroberflächen-Referenzhandbuch* enthalten sind.
- Planen der Ordnerstruktur (siehe Seite 372): Dieses vorhandene Thema wurde überarbeitet, um die Anforderungen für das Exportieren eines Ordners als vordefinierter Inhalt einzuschließen. Diese neue Exportmethode erfordert, dass sich alle Objekte für eine Release-Version im gleichen Ordner befinden.
- Vorbereiten der Produktionsumgebung für eine neue Version (siehe Seite 388): Dieser vorhandene Prozess wurde überarbeitet, um die neue Option zum Exportieren eines Ordners als vordefinierter Inhalt, die den Export von Automatisierungsobjekten des Typs "Paket" ersetzt, zu dokumentieren. Verwandte Themen sind:
  - Informationen zum Exportieren und Importieren von vordefinierten Inhalten (siehe Seite 388)
  - Szenario: Exportieren und Importieren von Objekten in einem Paket mit vordefiniertem Inhalt (siehe Seite 390) (Dieses Szenario umfasst ein Beispiel, Vorgänge und relevante Konzepte.)
- Bereinigen von Objekten und Ordnern (siehe Seite 409): Dieses vorhandene Thema wurde aktualisiert, um zu beschreiben, was geschieht, wenn Sie versuchen, ausgecheckte Objekte zu bereinigen. Diese Aktion wird ab CA Process Automation r4.2 neu unterstützt.

Inhalt

Kapitel 4: Verwalten erweiterter CA EEM-Sicherheit 75

Kapitel 5: Verwalten der CA Process Automation-Domäne 147

Kapitel 6: Verwalten von Umgebungen 167

Kapitel 7: Verwalten von Koordinationsrechnern 181

Kapitel 8: Verwalten von Agenten 209

Kapitel 9: Verwalten von Kontaktpunkten 235

Kapitel 13: Verwalten von Auslösern 335

Kapitel 14: Anwenderressourcen verwalten 349

Kapitel 15: Audit-Anwenderaktionen 359

Kapitel 16: Verwalten von Bibliotheksobjekten 371

Kapitel 1: Erste Schritte

Wenn Sie CA Process Automation erstmals mit CA EEM und einem internen Anwenderspeicher installieren, dann ist ein standardmäßiger Administratoranwender mit folgenden Anmeldeinformationen vorhanden:

Anwendername

pamadmin

Kennwort

pamadmin

Sie können zur neu installierten Produktinstanz navigieren und sich mit diesen Anmeldeinformationen anmelden. Eine bessere Vorgehensweise ist, ein Anwenderkonto während Ihrer ersten Sitzung in CA EEM zu erstellen und sich anschließend mit den definierten Anmeldeinformationen bei CA Process Automation anzumelden.

Konfigurieren Sie nach der Anmeldung die Einstellungen, mit denen die Sicherheit verwaltet und die Domäne konfiguriert wird.

Dieses Kapitel enthält folgende Themen:

Anmelden als EiamAdmin-Anwender in CA EEM

Der Anwender "EiamAdmin" kann sich bei CA EEM anmelden und Identitäten (Anwenderkonten) und Zugriffsrichtlinien verwalten.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zur URL für die CA EEM-Instanz, die CA Process Automation verwendet:

   `https://`*`Hostname`*`:5250/spin/eiam`

   hostname

   Definiert den Hostnamen oder die IP-Adresse des Servers, auf dem CA EEM installiert ist.

   Hinweis: Den Hostnamen von CA EEM, den CA Process Automation verwendet, finden Sie im Feld "CA EEM-Backend-Server" auf der CA Process Automation-Registerkarte "Konfiguration" der Unterregisterkarte "Sicherheit".

2. Wählen Sie in der Drop-down-Liste "Anwendung" den Wert aus, den Sie für den EEM-Anwendungsnamen während der Installation konfiguriert haben.

   Hinweis: Dies ist der Name, unter dem Sie CA Process Automation mit CA EEM registriert haben.

3. Geben Sie "**EiamAdmin**" und das Kennwort ein, das Sie für den EiamAdmin-Anwender angegeben haben.
4. Klicken Sie auf Anmelden.

Erstellen des ersten Administratorkontos

Sie können Ihr eigenes CA Process Automation-Anwenderkonto in CA EEM erstellen und vollen Zugriff (Administrator) auf CA Process Automation genehmigen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich als EiamAdmin-Anwender in CA EEM an (siehe Seite 16).
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Klicken Sie auf das Symbol neben "Anwender" im Auswahlmenü "Anwender".

   Die Seite "Neuer Anwender" wird angezeigt.

4. Geben Sie die Anwender-ID in das Namensfeld ein, die Sie als Anwendernamen eingeben möchten, wenn Sie sich bei CA Process Automation anmelden.
5. Klicken Sie auf "Anwendungsanwenderdetails hinzufügen".

6. Wählen Sie in "Verfügbare Benutzergruppen" "PAMAdmins" aus, und klicken Sie auf das Symbol ">", um sie in "Ausgewählte Benutzergruppen" zu verschieben.

   Die Gruppe gewährt vollständigen Zugriff auf alle Funktionen in CA Process Automation.

7. Geben Sie Ihre eigenen Details in den Abschnitt "Globaler Benutzer - Details" des Anwenderkontoprofils ein.
8. (Optional) Füllen Sie das Feld "Globale Gruppenmitgliedschaft" aus, wenn Sie CA Process Automation mit einem anderen CA Technologies-Produkt, das dieses CA EEM nutzt, verwenden.
9. Erstellen Sie das Kennwort im Abschnitt "Authentifizierung", das Sie eingeben möchten, wenn Sie sich bei CA Process Automation anmelden.
10. (Optional) Füllen Sie die verbleibenden Felder auf der Seite "Neuer Anwender" aus.
11. Klicken Sie auf "Speichern".

    Die Bestätigungsmeldung gibt "Globaler Benutzer erfolgreich erstellt" an. Anwendungsbenutzerdetails erfolgreich erstellt.

12. Klicken Sie auf "Schließen".
13. Klicken Sie auf "Abmelden".

Navigieren Sie zu CA Process Automation, und melden Sie sich an.

Die URL, die Sie verwenden, um auf CA Process Automation zuzugreifen, ist davon abhängig, ob der Domänen-Koordinationsrechner mit einem Knoten (nicht-geclustert) oder mit mehreren Knoten konfiguriert (geclustert) ist. Sie können direkt zu einem nicht-geclusterten CA Process Automation navigieren. Navigieren Sie für geclustertes CA Process Automation zum zugeordneten Lastenausgleich. Sie können alle Koordinationsrechner in der Domäne erreichen, indem die URL zum Domänen-Koordinationsrechner oder zum Lastenausgleich für den Domänen-Koordinationsrechner gestartet wird.

Gehen Sie folgendermaßen vor:

1. Durchsuchen Sie CA Process Automation.
   - Verwenden Sie für sichere Kommunikation die folgende Syntax:
     `https://`*`server`*`:`*`port`*`/itpam`

     Beispiele:
     `https://Orchestrator_host:8443/itpam`
     `https://loadBalancer_host:443/itpam`
   - Verwenden Sie für einfache Kommunikation die folgende Syntax:
     `http://`*`server`*`:`*`port`*`/itpam`

     Beispiele:
     `http://Orchestrator_host:8080/itpam`
     `http://loadBalancer_host:80/itpam`

   Die Anmeldeseite von CA Process Automation wird geöffnet.
2. Geben Sie die Anmeldeinformationen von Ihrem Anwenderkonto an.

   Hinweis: Wenn CA EEM so konfiguriert ist, um Anwender von mehreren Microsoft Active Directorys zu referenzieren und CA Process Automation Ihren uneingeschränkten Anwendernamen nicht akzeptiert, geben Sie Ihren Prinzipalnamen ein, d. h. *Domänenname\Anwendername*.
3. Klicken Sie auf Anmelden.

   CA Process Automation wird geöffnet. Die Registerkarte "Startseite" wird angezeigt.

Festlegen der Sprache und der Formate für Datum und Uhrzeit

Standardmäßig werden Datums- und Uhrzeitdaten für den Domänen-Koordinationsrechner in der Browserzeitzone angezeigt. Während Ihrer ersten Anmeldesitzung können Sie Ihre bevorzugten Datums-und Uhrzeitformate und die bevorzugte Sprache festlegen.

Hinweis: Das Produkt speichert alle Daten und Uhrzeiten in der koordinierten Weltzeit (Coordinated Universal Time, UTC).

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA Process Automation, und melden Sie sich an (siehe Seite 18), wenn Sie nicht bereits angemeldet sind.
2. Klicken Sie in der Symbolleiste auf Ihren Anwendernamen.
3. Wählen Sie im Dialogfeld "Anwendereinstellungen" Ihre bevorzugten Datums-und Uhrzeitformate aus.
4. Überprüfen und ändern Sie im Bedarfsfall die Spracheinstellung.
5. Klicken Sie auf Speichern und Schließen.
6. Klicken Sie auf OK.
7. Klicken Sie auf "Abmelden".

   Ihre Einstellungen werden übernommen, wenn Sie sich erneut anmelden.

Aktualisieren von vordefinierten Inhalten

Neue vordefinierte (standardmäßige) Inhalte sind regelmäßig verfügbar. Nur ein Administrator kann neue vordefinierte Inhalte importieren. Um sicherzustellen, dass der Ordner "PAM_PreDefinedContent" die aktuellsten vordefinierten Inhalte enthält, müssen Sie den Aktualisierungsvorgang gelegentlich wiederholen.

Gehen Sie folgendermaßen vor:

1. Löschen Sie zuvor importierten Inhalt.
   a. Klicken Sie auf die Registerkarte "Bibliothek".
   b. Wählen Sie den Ordner "PAM_PreDefinedContent" aus, klicken Sie auf "Löschen", und klicken Sie dann bei der Bestätigungsmeldung auf "Ja".

      Der Ordner "PAM_PreDefinedContent" wird in den Papierkorb verschoben. (Blenden Sie die Ordnerstruktur aus, um den Papierkorb anzuzeigen.)
   c. Wählen Sie den Ordner PAM_PreDefinedContent im Papierkorb aus, und klicken Sie auf Bereinigen.
2. Klicken Sie auf die Registerkarte Startseite.

3. Klicken Sie auf Durchsuchen von vordefinierten Inhalten.
4. Klicken Sie auf Ja, um den Import zu bestätigen.

   Der Importprozess erstellt den Ordner "PAM_PreDefinedContent" mit den aktuellsten Inhalten unter dem Stammverzeichnis der Registerkarte "Bibliothek".

Steuern des Zeitlimit-Intervalls

Sie können das Zeitlimit-Intervall des Produkts ändern. Standardmäßig wird das Produkt nach 15 Minuten Inaktivität automatisch abgemeldet.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich als ein Administrator am Server an, auf dem der Domänen-Koordinationsrechner installiert ist.
2. Wechseln Sie zum folgenden Ordner:

   `Installationsverzeichnis/server/c2o/.config`

   Installationsverzeichnis

   Gibt den Pfad an, wo der Domänen-Koordinationsrechner installiert ist.
3. Öffnen Sie die Datei "OasisConfig.properties" mit einem Editor.
4. Verwenden Sie "Suchen", um folgende Eigenschaft zu finden:

   `managementconsole.timeout`
5. Ändern Sie den Eigenschaftswert.
6. Speichern Sie die Datei, und schließen Sie den Editor.
7. Starten Sie den Koordinationsrechner-Service neu:
   a. Stoppen Sie den Koordinationsrechner (siehe Seite 206).
   b. Starten Sie den Koordinationsrechner (siehe Seite 207).

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Empfohlene IE-Browsereinstellungen für die NTLM-Durchleitungs-Authentifizierung

Die empfohlenen Windows Internet Explorer (IE)-Browsereinstellungen für die NTLM-Durchleitungs-Authentifizierung gelten in den folgenden Fällen, in denen CA EEM auf ein externes Active Directory verweist:

- CA EEM verwendet die NTLM-Durchleitungs-Authentifizierung, um globale CA Process Automation-Anwender zu authentifizieren.
- Anwender verwenden IE, um zu CA Process Automation zu navigieren.
- IE fordert zur Eingabe eines Anwendernamens und Kennworts auf.

Gehen Sie folgendermaßen vor:

1. Wählen Sie im IE aus dem Menü "Extras" den Menüpunkt "Internetoptionen" aus, und klicken Sie auf die Registerkarte "Sicherheit"
2. Wählen Sie das Symbol "Lokales Intranet" aus, und klicken Sie dann auf "Stufe anpassen".

   Das Dialogfeld "Sicherheitseinstellungen - Lokale Intranetzone" wird angezeigt.
3. Scrollen Sie zu "Benutzerauthentifizierung", und wählen Sie "Automatisches Anmelden nur in der Intranetzone" aus.
4. Fügen Sie die CA Process Automation-URL zur lokalen Intranetzone hinzu.

Informationen zu diesem Handbuch

Das *Handbuch für Inhaltsadministratoren* konzentriert sich auf Aufgaben, die Anwender in den folgenden Rollen ausführen:

- CA EEM-Administratoren, die CA EEM für CA Process Automation einrichten.
- CA Process Automation-Inhaltsadministratoren mit den Rechten "Domänenadministrator", "Umgebungskonfigurations-Administrator" und "Umgebungsinhalts-Administrator".

Zu den Aufgaben der Inhaltsadministratoren gehören:

- Einrichten der Sicherheit.
- Konfigurieren des Produkts zur Unterstützung der Entwicklung von Inhalten und Produktion.

Bevor Sie damit beginnen, dieses Handbuch zu verwenden, stellen Sie sicher, dass die Setup-Aufgaben im CA Process Automation-*Installationshandbuch* ausgeführt wurden.

Hinweise:

- Weitere Informationen zu Arbeitsabläufen, die sich auf das Einrichten einer neuen Inhaltsdesignumgebung oder einer neuen Produktionsumgebung beziehen, finden Sie in der *Online-Hilfe*.
- Weitere Informationen darüber, wie Inhaltsdesigner Webservices-Methoden verwenden, finden Sie im *Webservice-API-Referenzhandbuch*.
- Weitere Informationen darüber, wie Inhaltsdesigner Prozesse und andere Automatisierungsobjekte erstellen, finden Sie im *Handbuch für Inhaltsdesign.*
- Weitere Informationen über Operatoren finden Sie im *Referenzhandbuch für Inhaltsdesign*.
- Weitere Informationen darüber, wie Produktionsanwender das Produkt in einer Produktionsumgebung verwenden, finden Sie im *Produktionsanwenderhandbuch*.
- Weitere Informationen darüber, wie Designer während der Inhaltsgestaltung die Registerkarte "Vorgänge" verwenden, finden Sie im *Produktionsanwenderhandbuch*.

Kapitel 2: Übersicht für Administratoren

Dieses Kapitel enthält folgende Themen:

Übersicht über die Administrationsaufgaben

CA Process Automation stellt die primäre Schnittstelle für die Entwicklung von Inhalten dar. Systemadministratoren und Inhaltsadministratoren verwenden CA Process Automation für folgende Aktivitäten:

- Verwalten der Sicherheit.

  Für CA Process Automation umfasst die Sicherheit die Anwenderauthentifizierung bei der Anmeldung und rollenbasierten Zugriff. Sie definieren Anwenderkonten, anwenderspezifische Gruppen und Richtlinien, die Berechtigungen durch CA EEM gewähren.

- Verwalten der Domäne

  Domäne ist der Begriff, der zur Beschreibung der Unternehmensansicht des gesamten CA Process Automation-Systems, einschließlich Koordinationsrechnern, Agenten und Prozessbibliotheken, verwendet wird. Die Domänenverwaltung umfasst das Hinzufügen von Umgebungen, das gebündelte Entfernen nicht verwendeter Agenten und Kontaktpunkte und die Verwaltung von Domäneneigenschaften.

- Konfigurieren von Koordinationsrechnern

  Ein *Koordinationsrechner* ist die Engine-Komponente von CA Process Automation, die aus der Prozessbibliothek liest und Prozesse ausführt. Der erste CA Process Automation-Koordinationsrechner, den Sie installieren, ist der Domänen-Koordinationsrechner. Sie können dem Domänen-Koordinationsrechner für zusätzliche Verarbeitungsleistung und für den Lastenausgleich weitere Knoten hinzufügen. Wenn Ihre Anwender geografisch verteilt sind, sollten Sie Betracht ziehen, einen neuen standardmäßigen Koordinationsrechner in jedem Standort hinzuzufügen.

- Erstellen und Konfigurieren von Umgebungen.

  Eine *Umgebung* ist eine optionale Partition der Domäne, die die Entwicklung von Inhalten abgrenzt. Umgebungen können für Entwicklung, Tests und Produktion oder für verschiedene Geschäftsbereiche erstellt werden. Die Konfiguration umfasst das Hinzufügen von Kontaktpunkten und das Erstellen von Kontaktpunktgruppen.

- Konfigurieren von Agenten.

  Ein *Agent* ist eine CA Process Automation-Software, die Sie auf einem Netzwerkhost installieren. Koordinationsrechner, die Prozesse ausführen, können bestimmte Schritte des Prozesses auf Agentenhosts oder Remote-Hosts ausführen, zu denen die Agenten über SSH-Verbindungen verfügen. Die Konfiguration umfasst die Zuordnung von Kontaktpunkten, Proxy-Kontaktpunkten oder Hostgruppen zu Agenten.

- Zuordnen und Konfigurieren von Kontaktpunkten.

  Ein *Kontaktpunkt* ist eine logische Entität, die in Operatordefinitionen zur Darstellung des Zielagenten oder Zielkoordinationsrechners, durch den ein Teil des Prozesses ausgeführt werden soll, verwendet wird. Sie können einen Kontaktpunkt sofort mehreren Agenten und im Laufe der Zeit verschiedenen Agenten zuordnen. Kontaktpunkte bieten Flexibilität bei der Prozessimplementierung und reduzieren gleichzeitig den Wartungsaufwand für die Prozesse selbst.

- Zuordnen und Konfigurieren von Proxy-Kontaktpunkten und Hostgruppen

  Remote-Hosts, d. h. Hosts ohne installierten Agenten, können als Ziel festgelegt werden, um im Rahmen eines aktiven Prozesses Operationen auszuführen. Um Konnektivität zu ermöglichen, richten Sie den SSH-Zugriff auf den Remote-Host von einem Host mit einem Agenten ein. Auf dem Host mit dem Agenten konfigurieren Sie entweder einen Proxy-Kontaktpunkt oder eine Hostgruppe. Ein Operator kann auf einen Host mit dem Namen seines Proxy-Kontaktpunkts verweisen. Eine Hostgruppe verweist auf Remote-Hosts. Ein Operator kann mit seinem FQDN oder mit einer IP-Adresse auf so einen Remote-Host verweisen.

  Hinweis: Informationen finden Sie im Abschnitt für die Syntax für DNS-Hostnamen (siehe Seite 428).

- Durchsuchen Sie die Bibliothek.

  Eine *Bibliothek* ist das Repository, das Operator-Objekte und Skripte enthält, die von Inhaltsdesignern zum Erstellen von Prozessen zusammengestellt werden. Prozesse und andere Automatisierungsobjekte werden in der Bibliothek gespeichert.

- Verwalten von Automatisierungsobjekten in Bibliotheken

  Automatisierungsobjekte definieren Verarbeitung, Planung, Überwachung, Protokollierung und andere konfigurierbare Elemente eines CA Process Automation-Pakets. Automatisierungsobjekte werden in einer nicht geclusterten Architektur in einer Bibliothek eines bestimmten Koordinationsrechners gespeichert. Die Verwaltung von Automatisierungsobjekten umfasst die optionale Konfiguration von Sicherheitseinstellungen für einen Bibliotheksordner oder ein Objekt, um den Zugriff für bestimmte Gruppen und Anwender zu steuern.

- Verwalten von Sicherheit für Automatisierungsobjekte.

  Sie können anwenderspezifische CA EEM-Richtlinien für Automatisierungsobjekte erstellen. Aktivieren Sie zum Beispiel "Kontaktpunktsicherheit" und erstellen Sie in CA EEM Richtlinien zur Kontaktpunktsicherheit, um die Anwender zu beschränken, die bestimmte Operatoren auf angegebenen Zielen mit hohen Werten ausführen kann. Aktivieren Sie "Laufzeitsicherheit" und verwenden Sie die Option "Verantwortlichen festlegen", um nur dem Verantwortlichen des Prozesses die Rechte zum Starten eines Prozesses zu gewähren.

- Verwalten von Prozessen.

  Ein Beispiel für die Prozessverwaltung ist das Abbrechen fehlgeschlagener Prozesse mithilfe der Prozessüberwachung.

Übersicht über Registerkarten

Die Verfügbarkeit von bestimmten Registerkarten in der Benutzeroberfläche des Produkts hängt von den Zugriffsrechten ab, die angemeldeten Anwendern gewährt werden. Wenn Sie sich das erste Mal beim Produkt anmelden, zeigt die Benutzeroberfläche die Registerkarten an, die dieses Thema beschreiben.

Hinweis: Sie führen die meisten Konfigurations- und Administrationsaufgaben mithilfe der Registerkarte "Konfiguration" aus. Arbeitsabläufe, die sich auf die Registerkarte beziehen, finden Sie in der *Online-Hilfe*.

Startseite

Die Registerkarte "Startseite" bietet Ihnen schnellen Zugriff auf die Objekte, an denen Sie arbeiten. Sie können andere Verknüpfungen verwenden, um schnellen Zugriff auf allgemeine Informationen zu erhalten.

Bibliothek

Normalerweise erstellen Inhaltsadministratoren die Ordner und gewähren Zugriffsrechte dafür.

Hinweis: Inhaltsdesigner erstellen Objekte und greifen zur Bearbeitung auf die Objekte über die Registerkartenordner "Bibliothek" zu. Die Registerkarte "Designer" ist der Editor für Prozessobjekte.

Ordner

Ein Administrator richtet normalerweise eine Ordnerstruktur in der Designumgebung ein. Ordner enthalten Unterordner und Automatisierungsobjekte. Die empfohlene Vorgangsweise besteht darin, für jeden Prozess, den sie automatisieren, einen Ordner mit Unterordnern für alle Release-Versionen dieses Prozesses zu erstellen. Die Stammebene können Ordner auf Prozessebene sein.

Der Ordner, der die Release-Version eines Prozesses enthält, wird als vordefinierter Inhalt exportiert und danach in die Produktionsumgebung importiert. Der Importprozess erstellt die gleiche Ordnerstruktur in der Produktionsumgebung. Der Unterschied besteht darin, dass die Produktionsbibliothek nur die Release-Version des Prozesses und der verknüpften Objekte enthält. Ordner werden in der Produktionsbibliothek nicht manuell erstellt.

Papierkorb

Der Papierkorb im unteren Bereich des Koordinationsrechner-Knotens enthält Ordner und Objekte, die gelöscht wurden. Wenn Sie auf "Papierkorb" klicken, können Sie gelöschte Ordner und zu bereinigende (dauerhaft entfernen) Objekte aus der Bibliothek entfernen oder in der Bibliothek wiederherstellen.

Suchen

Definieren Sie Ordner, Schlüsselwörter oder Datumskriterien, die zur Suche nach Inhaltsobjekten im Suchfeld verwendet werden sollen.

Inhalt

Inhaltsdesigner erstellen Instanzen von ausgewählten Automatisierungsobjekten in einem Ordner. Sie öffnen die Instanzen, die vom Inhaltsteil der Registerkarte "Bibliothek" erstellt wurden.

Designer

Inhaltsdesigner entwerfen einen geplanten Prozess auf der Registerkarte "Designer".

Vorgänge

Die Registerkarte "Vorgänge" wird von Anwendern in der Gruppe "Produktionsanwender" verwendet. Es kann auf folgende Auswahlmenüs zugegriffen werden:

Links

Zeigt Informationen im rechten Bereich für folgende standardmäßige Links an:

Prozessinstanzen

Prozessinstanzen, die gestartet worden sind. Das Balkendiagramm im Bereich "Prozessinstanzen" zeigt Operatoren nach Zustand an. Der Bereich "Prozessinstanzen" zeigt auch Details für jeden Operator an.

Operatoren

Operatoren in gestarteten Prozessen und Aufgaben von Ablaufplänen. Das Balkendiagramm im Bereich "Operatoren" zeigt Operatoren nach Zustand an. Der Bereich "Operatoren" zeigt auch Details für jeden Operator an.

Tasks

Aufgaben, die Anwendern und Gruppen zugewiesen sind. Alle Anwender können ihre spezifischen Aufgabenliste und Aufgabenlisten für Gruppen, denen sie angehören, sowie anderen Anwendern zugewiesene Aufgaben anzeigen. Administratoren weisen den Anwendern oder Gruppen Aufgaben zu. Ein Anwender übernimmt eine zugewiesene Aufgabe und antwortet auf die Benachrichtigung der Anwenderinteraktion.

Aktive Ablaufpläne

Ablaufpläne, die aktive Prozesse gestartet haben.

Globale Ablaufpläne

Ablaufpläne, die alle Anwender verwenden können, um einen Prozess oder ausgewählte Operatoren zu starten. Sie können die Anzeige nach Datum, Koordinationsrechner oder Agentenkontaktpunkt und nach "Aktuell" oder "Archiviert" filtern.

Startaufträge

Aufträge zum Starten angegebener Prozesse nach Bedarf.

Vordefinierte Inhalte

Alle Anwender können Objekte überwachen, die als vordefinierter Inhalt in die Umgebung importiert werden. Wenn Sie auf ein Inhaltspaket im linken Bereich klicken, werden die Paketeigenschaften im rechten Bereich angezeigt.

Hinweis: Sie können die Informationen zur Release-Version für folgende Elemente anzeigen, die in Inhaltspaketen enthalten sind:

- Prozessinstanzen
- Aktive Ablaufpläne
- Globale Ablaufpläne
- Startaufträge

Das Produkt zeigt den Inhaltspaketnamen und das Inhaltspaket der Release-Version für jedes Objekt an.

Prozessüberwachung

Alle Anwender können Prozesse in allen Zuständen, aktiven Ablaufplänen, Operatoren, Startaufträge, Datensätze, Ressourcen und anwenderspezifische Operatoren überwachen.

Startaufträge

Anwender können ein Balkendiagramm von Instanzen der Startaufträge anzeigen, die in Warteschlange gestellt, ausgeführt, abgeschlossen und abgebrochen wurden. Für einen ausgewählten Balken können Anwender den Instanzennamen, die geplante Zeit, den Zustand, die Start- und Endzeit und den Anwendernamen anzeigen.

Datensatz

Anwender können die Struktur für einen ausgewählten Datensatz und die Namenswertpaare anzeigen.

Ressourcen

Anwender können ein Ressourcenobjekt auswählen und den rechten Bereich verwenden, um die angezeigten Werte in "Menge" und "In Verwendung" manuell zu überschreiben. Anwender können auch den Zustand ändern.

Ablaufpläne

Anwender können einen Ablaufplan auswählen und den rechten Bereich verwenden, um folgende Eigenschaften festzulegen:

- Das Ablaufdatum
- Die Aktivität wird entweder für alle Knoten oder für einen ausgewählten Koordinationsrechner angezeigt
- Gibt an, ob archivierte Ablaufpläne angezeigt werden

Konfiguration

Der Administrator, der für die Konfiguration von CA Process Automation verantwortlich ist, greift auf die Registerkarte "Konfiguration" zu. Umgebungen, Koordinationsrechner und Agenten erben standardmäßig die Einstellungen, die Administratoren auf Domänenebene konfigurieren. Operatoren übernehmen Einstellungen, die Administratoren auf Operatorkategorienebene konfigurieren. Die Registerkarte "Konfiguration" enthält folgende Auswahlmenüs:

Konfigurationsbrowser

Zeigt die folgenden Knoten an:

Domäne

Konfigurieren Sie die Domäne, die Standardumgebung, den Koordinationsrechner-Kontaktpunkt, die Agentenkontaktpunkte und Proxy-Kontaktpunkte sowie die Hostgruppen.

Koordinationsrechner

Konfigurieren Sie den Domänen-Koordinationsrechner und zusätzliche installierte Koordinationsrechner.

Agenten

Konfigurieren Sie Zuordnungen und Einstellungen für alle installierten Agenten.

Anwenderressourcen verwalten

Der Systemadministrator greift auf den Ordner "Anwenderressourcen" zu, um Skripten hinzuzufügen oder zu aktualisieren, die verwendet werden, um Inhalte zu entwickeln. Administratoren können JAR-Dateien in die Ordner "Agentenressourcen" und "Koordinationsrechnerressourcen" laden. Das Produkt gibt die hochgeladenen Dateien frei, wenn Sie Agenten oder Koordinationsrechner neu starten.

Installationen

Der Systemadministrator installiert weitere Koordinationsrechner oder Cluster-Knoten für den Domänen-Koordinationsrechner oder andere Koordinationsrechner. Administratoren installieren auch Agenten.

Berichte

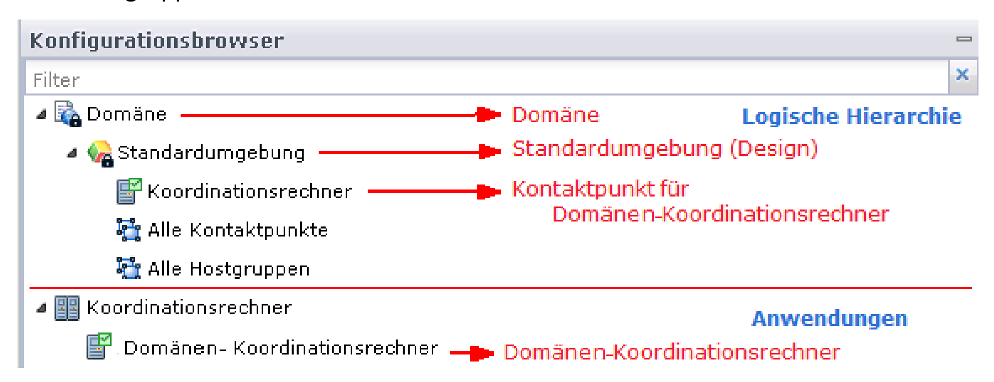
Alle Anwender können auf vordefinierte Berichte zugreifen oder anwenderspezifische Berichte hochladen, die von BIRT RCP Designer entworfen wurden.

Beziehungen zwischen Komponenten

Der Verantwortungsbereich eines CA Process Automation-Administrators umfasst:

- Konfiguration: Domäne, Standardumgebung oder Koordinationsrechner
- Installation und Konfiguration zur Einrichtung der Domäne: Andere Koordinationsrechner und Agenten.
- Erstellen und Konfigurieren logischer Entitäten: Umgebungen, Kontaktpunkte (einschließlich Proxy-Kontaktpunkte) und Hostgruppen.

Bevor Sie damit beginnen, ist es hilfreich, die Beziehungen zwischen diesen physischen und logischen Entitäten zu verstehen. Das Auswahlmenü "Konfigurationsbrowser" auf der Registerkarte "Konfiguration" zeigt eine Strukturanzeige der logischen Hierarchie, den Knoten "Koordinationsrechner" und den leeren Knoten "Agenten" an. Die logische Hierarchie besteht anfangs aus dem Knoten "Domäne" mit dem Knoten "Standardumgebung". Der eingeblendete Knoten "Standardumgebung" zeigt den Koordinationsrechner, den leeren Knoten "Alle Kontaktpunkte" und den leeren Knoten "Alle Hostgruppen" an.



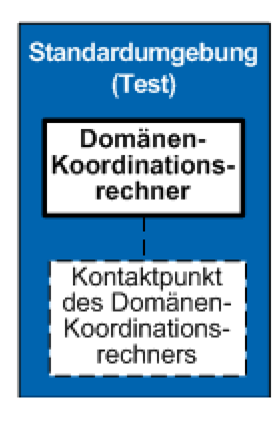
Die Domäne ist der Stammknoten der logischen Hierarchie. Alle Koordinationsrechner, die Sie installieren, werden unter dem Knoten "Koordinationsrechner" angezeigt. Alle Agenten, die Sie installieren, werden unter dem Knoten "Agenten" (nicht angezeigt) angezeigt.

Der Begriff "Kontaktpunkt" bezieht sich auf die Zuordnung zwischen einem Koordinationsrechner und einer Umgebung. Ein "Kontaktpunkt" bezieht sich auch auf die Zuordnung zwischen einem Agenten und einer Umgebung. Die Abbildung zeigt den Konfigurationsbrowser, der nach der ersten Installation von CA Process Automation sofort angezeigt wird. Deswegen enthält er keine Agenten oder Agentenkontaktpunkte. Inhaltsdesigner verwenden Kontaktpunkte als Ziele innerhalb der Prozesse, die sie automatisieren. (Auf die Verwendung und Vorteile von Kontaktpunkten wird an anderer Stelle näher eingegangen.)

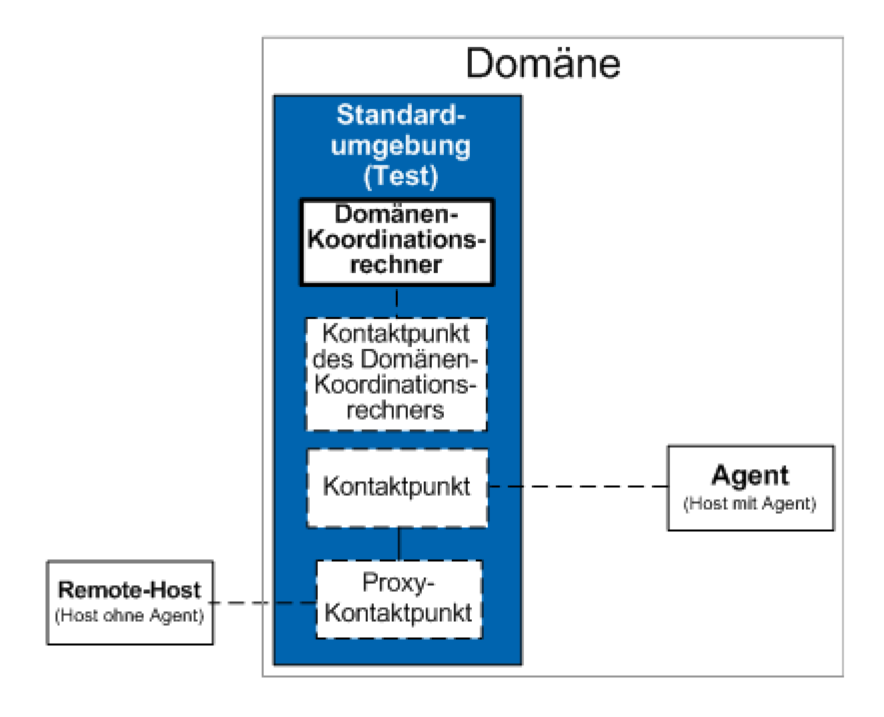
Die Standardumgebung ist normalerweise dem Design der automatisierten Prozesse zugewiesen. Inhaltsdesigner entwickeln Prozesse, die auf dem Kontaktpunkt des Domänen-Koordinationsrechners ausgeführt werden. Wenn der erste Prozess bereit für den Übergang zur Produktion ist, erstellen Sie eine neue Umgebung, und es wird eine "Produktionsumgebung" zur Domäne hinzugefügt.

Folgende Abbildung zeigt den Kontaktpunkt als Block mit einem gestrichelten Rahmen. Die Abbildung zeigt die Zuordnung zwischen dem Kontaktpunkt und dem Domänen-Koordinationsrechner als eine gestrichelte Linie.

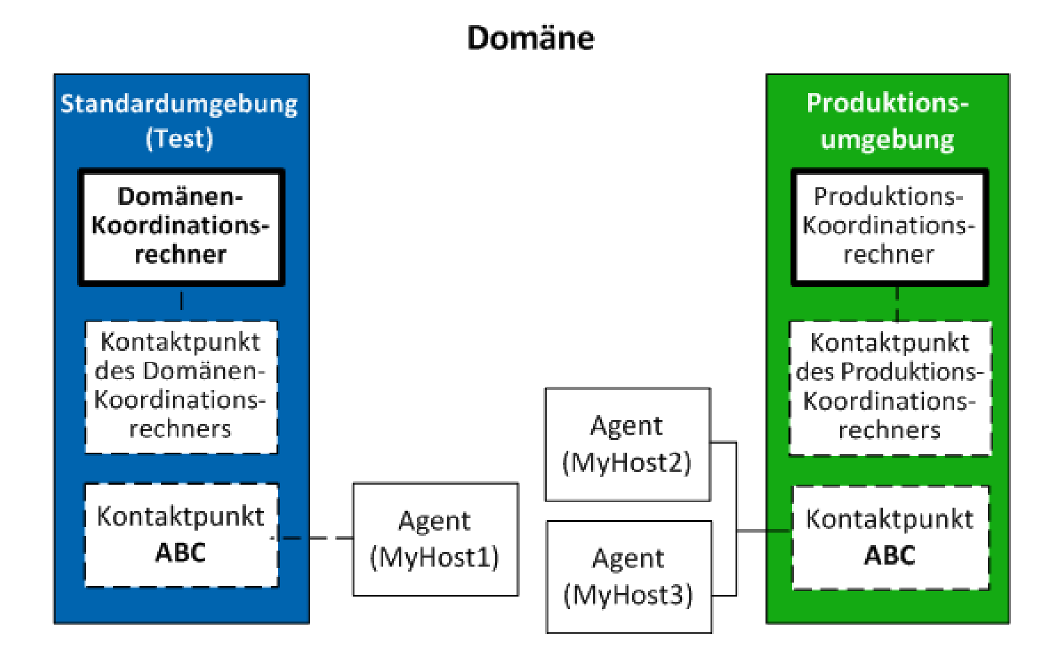
Domäne



Ein Prozess, der auf einem Koordinationsrechner ausgeführt wird, kann Operatoren enthalten, die auf andere Hosts abzielen müssen. Für solche Ziele ist es normalerweise erforderlich, dass Sie einen CA Process Automation-Agenten installieren und anschließend dem Agenten Kontaktpunkte zuordnen. Inhaltsdesigner greifen auf den Agenten über den Namen seines Kontaktpunkts zu. Wenn es nicht möglich ist, einen Agenten auf einem Zielhost zu installieren, werden Proxy-Kontaktpunkte verwendet. Ein *Proxy-Kontaktpunkt* erweitert die Kontaktpunktverwendung, sodass Koordinationsrechner Operatoren auf einem Remote-Host ausführen können (das bedeutet, auf einem Host ohne installierten Agenten). Wenn ein Kontaktpunkt mit einer SSH-Verbindung zwischen dem Agenten-Host und einem Remote-Host konfiguriert ist, dann ist der Kontaktpunkt ein Proxy-Kontaktpunkt.



Sie fügen für jeden Kontaktpunkt mit einer Zuordnung zur Designumgebung einen Kontaktpunkt mit dem gleichen Namen hinzu, und Sie ordnen der Produktionsumgebung den Kontaktpunkt zu. Ein Operator, der auf dem Kontaktpunkt ABC in der Designumgebung ausgeführt wird, wird auch auf einem Kontaktpunkt namens ABC in der Produktionsumgebung ausgeführt. In der Testumgebung kann der Kontaktpunkt zu einem einzelnen Agenten zugeordnet werden. Um Hochverfügbarkeit in der Produktionsumgebung zu unterstützen, kann der Kontaktpunkt zu zwei Agenten zugeordnet werden.



Weitere Informationen:

Informationen über Domänenhierarchie, Koordinationsrechner und Agenten (siehe Seite 162)

Kardinalität von Komponentenzuordnungen

Als CA Process Automation-Administrator richten Sie die Domäne ein, indem Sie Koordinationsrechner und Agenten installieren. Sie partitionieren die Domäne, indem Sie Umgebungen erstellen, wo jede Umgebung eine eigene Bibliothek hat.
Sie konfigurieren Kontaktpunkte für Inhaltsdesigner, um Ziele für Operatoren anzugeben. Klicken Sie auf die Registerkarte "Konfiguration", und öffnen Sie das Auswahlmenü "Konfigurationsbrowser", um diese Entitäten anzuzeigen.

Die folgenden Regeln bestimmen die Kardinalität zwischen Entitätspaaren, die zueinander zugeordnet sein können:

Domäne, Umgebungen, Koordinationsrechner, Agenten

Koordinationsrechner und Agenten sind Softwarekomponenten, die *physisch* auf Hosts installiert werden. Die Domäne und Umgebungen sind *logische* Entitäten.

- Ein CA Process Automation-System hat nur eine Domäne.
- Wenn ein neues CA Process Automation-System installiert wird, hat die Domäne eine Standardumgebung. Die Standardumgebung enthält den Domänen-Koordinationsrechner.
- Die Domäne kann zahlreiche Umgebungen aufweisen. Sie können Umgebungen getrennten Bibliotheken hinzufügen. Zum Beispiel können Sie die Standardumgebung verwenden, um neue Inhalte zu gestalten und zu testen. Danach können Sie eine separate Produktionsumgebung erstellen. Jede Umgebung muss mindestens über einen Koordinationsrechner verfügen.

  Hinweis: Normalerweise exportiert ein Administrator Inhalte aus der Standardumgebung und importiert sie anschließend in die Produktionsumgebung. Sie können Inhalte auch domänenübergreifend übertragen.
- Eine Umgebung kann einen oder mehrere Koordinationsrechner aufweisen. Jeder Koordinationsrechner wird auf einem separaten Host installiert.

  Hinweis: Ein Koordinationsrechner kann *standardmäßig* oder *geclustert* sein. Ein geclusterter Koordinationsrechner hat mehrere Knoten. Jeder Knoten wird auf einem separaten Host installiert. Ein Koordinationsrechner wird im Konfigurationsbrowser als einzelne Entität angezeigt, unabhängig davon, ob es sich um einen geclusterten oder einen standardmäßigen (nicht geclustert) Koordinationsrechner handelt.
- Die Domäne kann so viele Agenten aufweisen, wie Sie benötigen. Agenten werden auf Hosts installiert und sind von Umgebungen unabhängig.

Umgebungen und Kontaktpunkte

Umgebungen und Kontaktpunkte sind *logische* Entitäten.

- Jeder Kontaktpunkt gehört zu einer Umgebung.
- Jede Umgebung kann zahlreiche Kontaktpunkte aufweisen.
- Für jeden Kontaktpunkt, der in einer Release-Version eines Prozesses in der Designumgebung verwendet wird, muss ein gleichnamiger Kontaktpunkt in der Produktionsumgebung vorhanden sein. Dadurch kann der nicht änderbare Prozess in der Produktionsumgebung ausgeführt werden.

Koordinationsrechner und Kontaktpunkte

Nachdem Sie einen Koordinationsrechner installiert haben, erstellen Sie einen Kontaktpunkt, der dem Koordinationsrechner mit einer bestimmten Umgebung zugeordnet ist. Operatoren in einem Prozess verwenden den Kontaktpunkt, der dem Koordinationsrechner zugeordnet ist, als Ziel. Die Kontaktpunkt-Zuordnung bestimmt die Umgebung, in der der Prozess ausgeführt wird.

- Der Domänen-Koordinationsrechner verfügt über einen vordefinierten Kontaktpunkt.
- Jeder Koordinationsrechner wird nur einem Kontaktpunkt zugeordnet.
- Ein Kontaktpunkt, der einem Koordinationsrechner zugeordnet ist, kann einem Agenten nicht zugeordnet werden. Verbindungen von Kontaktpunkt zu Koordinationsrechner und von Kontaktpunkt zu Agent schließen sich gegenseitig aus.
- Ein Operator wird auf dem Koordinationsrechner-Kontaktpunkt ausgeführt, der den Prozess ausführt, wenn das Operatorziel leer ist.

Agenten und Kontaktpunkte

Um einen Agenten für einen Operator als Ziel verfügbar zu machen, ordnen Sie den Agenten zu einem Kontaktpunkt, einem Proxy-Kontaktpunkt oder einer Hostgruppe zu.

- Sie können einen Agenten zu einem oder mehreren Kontaktpunkten zuordnen.
  - Wenn Sie einen Agenten zu einem Kontaktpunkt zuordnen, können Operatoren direkt auf einem Host mit einem installierten Agenten ausgeführt werden, indem der Kontaktpunkt als Ziel verwendet wird.
  - Wenn Sie einen Agenten zu mehreren Kontaktpunkten auf dem gleichen Host zuordnen, sind die Ziele der Kontaktpunkte üblicherweise unterschiedliche Komponenten auf dem Host. Zum Beispiel könnten Sie einen Kontaktpunkt definieren, um auf eine Datenbank zuzugreifen, und einen weiteren, um auf ein Drittanbieterprodukt zuzugreifen.
  - Jeder Operator in einem Prozess wird auf einem Kontaktpunkt ausgeführt. Dieser Kontaktpunkt kann zu einem Operator, einem Agenten oder mehreren Agenten zugeordnet werden. Wenn Operator 1 auf dem Kontaktpunkt ABC in der Design- oder Testumgebung ausgeführt wird, wird er auf einem Kontaktpunkt namens ABC in der Produktionsumgebung ausgeführt. Alle Mitglieder dieses Kontaktpunktpaares sind zu unterschiedlichen Umgebungen zugeordnet. Die Mitglieder des Kontaktpunktpaares können zu demselben Agenten oder anderen Agenten zugeordnet sein. Dieser Zuordnungstyp ist ein Mechanismus für die Definition von Prozessen, die Sie umgebungsübergreifend migrieren können, ohne die Zielhostinformationen ändern zu müssen.
- Sie können einen Kontaktpunkt zu einem oder mehreren Agenten zuordnen. Sie können mehreren Agenten die gleiche Priorität zuweisen oder jedem Agenten eine unterschiedliche Priorität zuweisen.
  - Wenn die Agenten unterschiedliche Prioritäten haben, werden Operatoren auf dem Agenten mit der höchsten Priorität ausgeführt. Wenn der Agent mit der höchsten Priorität nicht verfügbar ist, werden die Operatoren auf einem verfügbaren Agenten mit einer niedrigeren Priorität ausgeführt. Dieses Design stellt sicher, dass ein Zielhost verfügbar ist.
  - Wenn einem Kontaktpunkt mehrere Agenten mit derselben Priorität zugeordnet sind, werden Operatoren auf einem nach dem Zufallsprinzip ausgewählten Agenten ausgeführt. Dieses Design fördert den Lastenausgleich.
  - Ein Kontaktpunkt, der einem Koordinationsrechner zugeordnet ist, kann einem Agenten nicht zugeordnet werden.

Agenten, Proxy-Kontaktpunkte und Remote-Hosts

Ein Remote-Host ist ein Host, der ein Operatorziel ist, wenn es nicht praktisch ist, einen Agenten zu installieren.

- Sie können einen Agenten zu einem oder mehreren Proxy-Kontaktpunkten zuordnen.
- Ein *Proxy-Kontaktpunkt* ist ein Kontaktpunkt, der mit einer SSH-Verbindung zu einem Remote-Host konfiguriert wird. Der Remote-Host verfügt normalerweise nicht über einen Agenten.
- Wenn Sie einen Agenten zu einem Proxy-Kontaktpunkt zuordnen, können Operatoren in einem Prozess den Proxy-Kontaktpunkt als Ziel haben, auf dem Remote-Host ausgeführt zu werden.

Hinweis: Durch die Verwendung des Operators "SSH-Skript ausführen" in einem Prozess kann ein Koordinationsrechner die Auslastung ohne Umwege über einen Agenten an einen Remote-Host verteilen. Der Inhaltsdesigner definiert (im Operator) Konfigurationsparameter, die Hostadresse und Anmeldeinformationen für die SSH-Verbindung mit dem Remote-Host und die Ausführung eines Skripts festlegen. Details zum Operator "SSH-Skript ausführen" finden Sie im *Referenzhandbuch für Inhaltsdesign*.

Agenten, Hostgruppen und Remote-Hosts

Eine *Hostgruppe* ist eine Gruppe von Remote-Hosts. Sie konfigurieren normalerweise Hostgruppen mit einem gemeinsamen Muster für Hostnamen oder mit einem IPv4-Teilnetz, das in der CIDR-Notation ausgedrückt ist.

- Sie können einen Agenten zu einer oder mehreren Hostgruppen zuordnen.
- Sie können eine Hostgruppe zu einem oder mehreren Agenten zuordnen.
- Wenn ein Agent zu einer Hostgruppe zugeordnet ist, konfigurieren Sie die SSH-Verbindungen manuell. Konfigurieren sie manuell jeweils eine SSH-Verbindung vom Agenten-Host zu jedem Remote-Host, der von der Hostgruppe referenziert wird.
- Wenn ein Agent einer Hostgruppe zugeordnet ist, werden Operatoren in einem Prozess auf einem referenzierten Remote-Host ausgeführt. Operatoren zielen auf die IP-Adresse oder FQDN des Remote-Hosts ab.

Hinweis: Verwenden Sie für nicht interaktive SSH-Kommunikation mit einem Remote-Host einen Proxy-Kontaktpunkt oder eine Hostgruppe. Verwenden Sie für interaktive SSH-Kommunikation mit einem Remote-Host den Operator "SSH-Skript ausführen". Details zum Operator "SSH-Skript ausführen" finden Sie im *Referenzhandbuch für Inhaltsdesign*.

Sicherheit

Als Administrator können Ihre Überlegungen zur Sicherheit von CA Process Automation folgende Aspekte umfassen:

- Sichern der CA Process Automation-Anwendung (siehe Seite 39).
- Deaktivieren eines Anwenderkontos (siehe Seite 40).
- Sichern des Datentransfers mit starken Chiffrierungen (siehe Seite 41).
- Sichern des Datentransfers zwischen CA Process Automation und CA EEM (siehe Seite 41).

Weitere Informationen:

Verwalten der grundlegenden CA EEM-Sicherheit (siehe Seite 43)

Sichern der CA Process Automation-Anwendung

Ein Grund für das Sichern der Anwendung ist, das Anmelden von nicht autorisierten Anwendern zu verhindern. Ein anderer Grund ist, die Verwendung der Funktion basierend auf der Rolle des angemeldeten Anwenders zu beschränken. Das Sichern der Anwendung umfasst folgende Mechanismen:

Authentifizierung

Das Produkt verwendet CA EEM, um Anwender bei der Anmeldung zu authentifizieren. CA EEM vergleicht die Anmeldeinformationen, die Anwender bei der Anmeldung mit Anwendernamen und Kennwortkombinationen in den Anwenderkonten eingeben. Der Anwender kann sich nur anmelden, wenn CA EEM eine Übereinstimmung findet.

Administratoren können das Produkt vor unbefugten Anmeldungen schützen, indem sie Anwender dazu auffordern, ihre Kennwörter regelmäßig zu ändern, und indem sie Standardkonten deaktivieren. Weitere Informationen finden Sie hier:

- Ändern des eigenen Kennworts in CA EEM (siehe Seite 47)
- Deaktivieren eines Anwenderkontos (siehe Seite 40)

Autorisierung und rollenbasierte Sicherheit

Das Produkt verwendet CA EEM, um angemeldete Anwender zu autorisieren. CA EEM ermöglicht es Anwendern, Aufgaben nur auf den Teilen der Anwenderoberfläche auszuführen, zu der sie autorisiert sind. Autorisierung für die Gruppe "PAMAdmins", "Designer" und "Produktionsanwender" ist standardmäßig festgelegt. Anwender, die diesen Gruppen hinzugefügt sind, übernehmen die Autorisierung.

Administratoren können rollenbasierte Sicherheit definieren, sodass Anwender, die zu verschiedenen Gruppen gehören, nur auf Teile des Produkts zugreifen, die für die von ihnen ausgeführte Rolle notwendig sind. Administratoren können auch CA EEM-Richtlinien verwenden, um vertrauenswürdige Anwender zu Aktivitäten zuzuweisen, bei denen Missbrauch den größten Schaden verursachen kann. Dieser Aspekt der Zugriffssteuerung ist eine Überlegung, die getrennt von der Gruppenrolle erfolgt, der einzelne Anwender zugewiesen sind.

Weitere Informationen:

Authentifizierung und Autorisierung von Anwendern im FIPS-Modus (siehe Seite 413)

Deaktivieren eines Anwenderkontos

Sie können ein Anwenderkonto in den folgenden Fällen deaktivieren:

- Der Anwender benötigt keinen Zugriff auf CA Process Automation mehr, aber der Anwenderdatensatz muss zu Auditing-Zwecken beibehalten werden.
- Sie müssen aus bestimmten Gründen vorübergehend oder dauerhaft verhindern, dass der angegebene Anwender auf CA Process Automation zugreift.
- Die vordefinierten Anmeldeinformationen, die Ihnen bei der Installation zur Verfügung gestellt wurden, stellen jetzt eine interne Sicherheitsbedrohung dar. Da die Anmeldeinformationen für die Anwender "pamadmin" und "pamuser" dokumentiert sind, empfiehlt es sich, diese unzugänglich zu machen, nachdem sie ihren Zweck erfüllt haben.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei CA EEM an.
2. Klicken Sie auf "Identitäten verwalten".
3. Wählen Sie unter "Search Users" die Option "Application User Details" aus, und klicken Sie auf "Los".
4. Klicken Sie auf den Namen des Zielanwenders.
5. Führen Sie einen Bildlauf zum Abschnitt "Authentifizierung" durch, und führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf "Suspended".
   - Klicken Sie auf "Disable Date", wählen Sie das Datum aus, an dem die Deaktivierung wirksam werden soll, und klicken Sie auf "OK".
6. Klicken Sie auf "Speichern".

Hinweis: Sie können die Deaktivierung auch rückgängig machen oder ein deaktiviertes Konto aktivieren. Sie können die Deaktivierungs-/Aktivierungsfunktion verwenden, um die Verfügbarkeit eines neuen Kontos bis zu dem von Ihnen angegebenen Zeitpunkt aufzuschieben.

Sichern des Datentransfers mit starken Chiffrierungen

Wenn CA Process Automation-Komponenten auf Java Virtual Machine installiert sind, ermöglichen JVMs, wie z. B. Java 6, mittelmäßige und schwache Verschlüsselungen bei Kommunikationen mit Agenten. Um diese Kommunikationen zu sichern, fügen Sie starke Chiffrierungswerte zur Eigenschaftsdatei "Oasis.Config" im folgenden Verzeichnis hinzu:

```
Installationsverzeichnis\server/c2o\config\
```

Folgende Eigenschaften beziehen sich auf Verschlüsselungen, die in SSL-Kommunikation verwendet werden:

jboss.ssl.ciphers

Gibt eine durch Kommas getrennt Liste mit Verschlüsselungen an, die für die SSL-Kommunikation zwischen dem Domänen-Koordinationsrechner und Clients, wie z. B. Browser und Webservices, verwendet werden sollen. Die Chiffrierungsliste kann nach dem Betriebssystem und der JVM, das bzw. die auf dem Host vorhanden ist, variieren. Folgendes Beispiel zeigt eine normale Spezifikation von starken JBoss-Verschlüsselungen:

```
jboss.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DS
S_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE
_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA
```

jetty.ssl.ciphers

Gibt eine durch Kommas getrennte Liste mit Verschlüsselungen an, die für die SSL-Kommunikation mit Agenten verwendet werden sollen. Das Produkt fügt während der automatischen Installation Agenten diese Eigenschaft hinzu. Folgendes Beispiel zeigt eine normale Spezifikation von Jetty-Verschlüsselungen:

```
jetty.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA
```

Sichern des Datentransfers zwischen CA Process Automation und CA EEM

CA Process Automation verwendet Verschlüsselung, um gespeicherte und übertragene Daten zu sichern. Wenn der CA EEM-FIPS-Modus aktiviert ist, sichert CA Process Automation gespeicherte und übertragene Daten mit FIPS-140-2 validierten kryptografischen Modulen.

Arten der Authentifizierung

CA EEM authentifiziert und autorisiert alle Anwender, die zu CA Process Automation navigieren. CA EEM kann Anwender folgendermaßen authentifizieren:

- Verwenden Sie die Anmeldeinformationen, die Anwender in ein formularbasiertes Anmeldedialogfeld eingeben.
- Verwenden Sie das NTLM-Protokoll, wenn NTLM-Durchleitungs-Authentifizierung konfiguriert ist. Diese Funktion wird oft ausgewählt, wenn CA EEM zur Verwendung von Microsoft Active Directory als externes Verzeichnis konfiguriert ist. Die Anmeldeinformationen werden für diese Konfiguration automatisch in CA EEM geladen.

Wenn ein Anwender zu CA Process Automation navigiert, bestimmt der Koordinationsrechner den Authentifizierungstyp, der verwendet werden soll:

Formularbasiert

Die Anmeldeseite von CA Process Automation wird geöffnet. Der Anwender gibt Anmeldeinformationen ein, und das Anmeldeverfahren beginnt.

NTLM

Das NTLM-Protokoll authentifiziert den Anwender zum CA EEM-Server, und die Startseite wird geöffnet.

Kapitel 3: Verwalten der grundlegenden CA EEM-Sicherheit

Wenn Sie CA Process Automation installieren oder ein Upgrade durchführen, wird CA Process Automation mit CA EEM registriert. CA EEM bietet für zahlreiche CA Technologies-Produkte Services für die Zugriffsrichtlinien-Verwaltung, Authentifizierung und Autorisierung. Die Sicherheitsverwaltung variiert je nachdem, ob Sie die Sicherheitseinstellungen das erste Mal einrichten oder ob Sie ein Upgrade von CA Process Automation durchgeführt haben. Wenn Sie ein Upgrade durchführen, hängen die Sicherheitsanforderungen davon ab, ob Sie vorher CA EEM oder LDAP zur Anwenderauthentifizierung verwendet haben. Unabhängig davon, ob Sie ein neuer Anwender sind oder ein Upgrade durchführen, wenn Sie Anwenderkonten von einem externen Verzeichnisserver in CA EEM laden möchten, ist eine separate Reihe von Prozeduren erforderlich.

Dieses Kapitel befasst sich mit der Verwendung von CA EEM, um jeden Anwender eine von vier Standardrollen zuzuweisen, unabhängig davon, ob Sie Anwenderkonten erstellen, über vorhandene Anwenderkonten verfügen oder Anwenderkonten aus einem externen Verzeichnis laden.

Weitere Informationen finden Sie unter Verwalten erweiterter CA EEM-Sicherheit (siehe Seite 75), wenn Sie anwenderdefinierte Rollen und anwenderdefinierte Richtlinien erstellen.

Dieses Kapitel enthält folgende Themen:

Bestimmen des Prozesses für das Erhalten von rollenbasiertem Zugriff

Sicherheitsverwaltung mit CA EEM variiert für die folgenden Szenarien:

- Neue Installation oder Upgrade der Installation mit einem referenzierten Verzeichnisserver: Sie haben CA EEM so konfiguriert, dass die Authentifizierung auf Anmeldeinformationen basiert, die in CA EEM als globale Anwenderkonten von einem externen Anwenderspeicher geladen werden. Sie können nun eine Anwendungsgruppe einem beliebigen globalen Anwender zuzuweisen, der die ausgeführte Rolle in CA Process Automation widerspiegelt.
- Neue Installation mit einem lokalen CA EEM: Sie können nun CA Process Automation-Anwender in CA EEM definieren.
- Upgrade der Installation, bei der Sie vorher CA EEM verwendet haben: Sie können Anwenderkonten für Anwender aktualisieren, die Prozesse entwerfen oder die Prozesse verwenden, die zur Produktionsumgebung übertragen wurden. Öffnen Sie jedes Konto und wählen Sie eine der neuen Anwendungsgruppen aus: Designer oder Produktionsanwender.
- Upgrade-Installation, bei der Sie zuvor Microsoft Active Directory oder einen ähnlichen LDAP-Server verwendeten. Sie können nun Anwenderkonten Ihrer vorhandenen Anwender in CA EEM erstellen. Sie können entweder den Anwendern eine Standardgruppe zuweisen oder Sie können anwenderspezifische Gruppen erstellen, mit denen Sie die Rollen, die Sie mit AD verwendet haben, beibehalten können.

Bestimmen des Prozesses für den Erhalt rollenbasierten Zugriffs

CA EEM-Administrator

Ext. Anwender-speicher ver-wenden?

Ja

Verwalten des Zugriffs für referenzierte Anwenderkonten

Nein

Neu?

Ja

Erstellen von Anwender-konten mit Standardrollen

Nein

CA EEM zuvor verwendet?

Ja

Aktualisieren von Anwender-konten mit Standardrollen

Nein

AD zuvor verwendet?

Ja

AD-Rechte beibehalten?

Nein

Ja

Erstellen von Anwender-konten mit benutzerde-finierten AD-Rollen

Basierend auf dem Ergebnis des Entscheidungsdiagramms gehen Sie zum entsprechenden Abschnitt:

- Verwalten der Zugriffe für referenzierte Anwenderkonten (siehe Seite 62).
- Anwenderkonten mit Standardrollen erstellen (siehe Seite 55).
- Aktualisieren von Anwenderkonten mit Standardrollen (siehe Seite 61).
- Erstellen von Anwenderkonten mit anwenderspezifischen AD-Rollen.

  Weitere Informationen finden Sie unter So führen Sie eine Transition von in Active Directory verwendete Rollen zu CA EEM durch (siehe Seite 119).

Navigieren Sie zu CA EEM, und melden Sie sich an.

Um Anwender, Anwendergruppen und Richtlinien zu verwalten, die Berechtigungen in CA Process Automation gewähren, melden Sie sich bei der konfigurierten Anwendung in CA EEM an.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, das CA Process Automation verwendet. Verwenden Sie folgende URL:

   `https://`*`Hostname`*`:5250/spin/eiam`

   Das CA Embedded Entitlements Manager-Dialogfeld wird geöffnet.

2. Wählen Sie in der Drop-down-Liste "Anwendung" den Namen aus, der bei der Installation im Feld "EEM-Anwendungsname" konfiguriert wurde.

   Hinweis: Der Standardname ist "Process Automation".

3. Geben Sie eine der folgenden Anmeldeinformationen ein:

   - Geben Sie **EiamAdmin** und das CA EEM-Administratorkennwort ein, das während des Installationsprozesses eingerichtet wurde.
   - Geben Sie Ihren Anwendernamen und Ihr Kennwort ein, wenn der CA EEM-Administrator Ihnen den CA EEM-Zugriff gewährt hat. Der CA EEM-Administrator kann ausgewählten Administratoren CA EEM-Zugriff gewähren (siehe Seite 77).

4. Klicken Sie auf Anmelden.

Verwenden von CA EEM zur Änderung Ihres CA Process Automation-Kennworts

Der Administrator weist normalerweise ein temporäres Kennwort zu, wenn Anwenderkonten für den internen Anwenderspeicher eingerichtet werden. Alle CA Process Automation-Anwender mit Anwenderkonten, die in CA EEM erstellt wurden, können dieses Kennwort ändern, bevor Sie sich bei CA Process Automation anmelden. Dann können Sie Ihr CA Process Automation-Kennwort im Intervall ändern, das von Kennwortrichtlinien angegeben wird.

Hinweis: Diese Möglichkeit gilt nicht, wenn CA EEM auf Anwenderkonten von einem externen Anwenderspeicher wie Microsoft Active Directory verweist. Verwalten Sie in diesem Fall Ihr Kennwort innerhalb des referenzierten Verzeichnisses.

Verwenden Sie CA EEM, um Ihr CA Process Automation-Kennwort zu ändern.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie einen Browser, und geben Sie die URL für den von CA Process Automation verwendete CA EEM-Server ein. Zum Beispiel:
   `https://`*`Hostname_oder_IP-Adresse`***`:5250/spin/eiam/`**

   Den Hostnamen oder die IP-Adresse von CA EEM, den CA Process Automation verwendet, finden Sie im Feld "CA EEM-Backend-Server" auf der CA Process Automation-Registerkarte "Konfiguration" der Unterregisterkarte "Sicherheit".

2. Melden Sie sich bei CA Embedded Entitlements Manager (CA EEM) über das Dialogfeld "Anmelden" an:

   a. Wählen Sie für Anwendung <Global> aus.

   b. Löschen Sie EiamAdmin, wenn dieser Standardname im Feld Benutzername angezeigt wird.

   c. Geben Sie Ihren Anwendernamen und Ihr Kennwort für CA Process Automation ein.

   d. Klicken Sie auf Anmelden.

3. Klicken Sie unter Selbstverwaltung auf Kennwort ändern.

4. Setzen Sie Ihr Kennwort zurück:

   a. Geben Sie Ihre Anwenderdaten und Ihr Kennwort für CA Process Automation ein.

   b. Geben Sie Ihr neues Kennwort in die Felder "Neues Kennwort" und "Kennwort bestätigen" ein.

   c. Klicken Sie auf OK.

   Wenn Sie sich bei CA Process Automation anmelden, werden Ihre aktualisierten Anmeldeinformationen akzeptiert.

Rollenbasierter Zugriff auf Konfiguration

Rollenbasierter Zugriff wird in CA EEM implementiert, wo PAMAdmins (für Administratoren), Designer und Produktionsanwender drei anwendungsspezifische Gruppen sind. Jeder Gruppe werden Berechtigungen zugeteilt, sodass die Mitglieder nur auf die Funktionalität zugreifen können, die zur entsprechenden Rolle gehört. Die vierte Standardgruppe, PAMUsers, kann, wenn anwendbar, als Grundlage für anwenderspezifische Gruppen verwendet werden.

PAMAdmins (Administratoren)

Administratoren haben vollständigen Zugriff auf die Registerkarte "Konfiguration". Administratoren konfigurieren Einstellungen auf allen Ebenen der Domänenhierarchie. Die Auswahlmenüs "Installation" und "Anwenderressourcen verwalten" werden auf der Registerkarte "Konfiguration" nur für Anwender angezeigt, die Administratoren sind.

Designer

CA EEM ermöglicht es den Anwendern in der Gruppe "Designer", den Konfigurationsbrowser und die Konfigurationseinstellungen auf Registerkarte "Konfiguration" anzuzeigen. Inhaltsdesigner können prüfen Sie, ob bestimmte Agenten fehlgeschlagen sind oder ob eine bestimmte Kategorie von Operatoren auf einem angegebenen Kontaktpunkt deaktiviert ist.

Produktionsanwender

CA EEM erlaubt es Anwendern in der Produktionsanwender-Gruppe, die Registerkarte "Konfiguration" anzuzeigen.

Standardgruppen und Anmeldeinformationen von Standardanwendern

CA EEM stellt vier Standardgruppen für CA Process Automation bereit. Jede Gruppe hat einen Standardanwender. CA Process Automation wird Mitgliedern jeder Gruppe präsentiert, indem die Anmeldung an CA Process Automation als Standardanwender erfolgt. Es folgen detaillierte Beschreibungen und Anmeldeinformationen für Standardanwender:

PAMAdmins

Die PAMAdmins-Gruppe erhält volle Berechtigungen in CA Process Automation. Sie können diese Gruppe allen Administratoren zuweisen.

Standard-Anwenderanmeldeinformationen

Anwendername: pamadmin

Kennwort: pamadmin

Designer

Der Designer-Gruppe werden Berechtigungen erteilt, die normalerweise ausreichend für Anwender sind, die automatische Prozesse entwerfen.

Standard-Anwenderanmeldeinformationen

Anwendername: pamdesigner

Kennwort: pamdesigner

Produktionsanwender

Der Produktionsanwender-Gruppe werden hinreichende Berechtigungen für Anwender erteilt, die mit automatischen Prozessen in der Produktionsumgebung interagieren.

Standard-Anwenderanmeldeinformationen

Anwendername: pamproduser

Kennwort: pamproduser

PAMUsers

Der Standard-PAMUsers-Gruppe werden minimale Berechtigungen erteilt. Der CA EEM-Administrator kann diese Gruppe als Grundlage für anwenderspezifische Gruppen verwenden. Diese Gruppe ermöglicht es, sich bei CA Process Automation anzumelden, Berichte zu prüfen und den Zustand von Betriebsabläufen anzuzeigen.

Standard-Anwenderanmeldeinformationen

Anwendername: pamuser

Kennwort: pamuser

Es folgen detaillierte Berechtigungsbeschreibungen:

- PAMAdmins-Gruppenberechtigungen (siehe Seite 50).
- Designer-Gruppenberechtigungen (siehe Seite 51).
- Produktionsanwender-Gruppenberechtigungen (siehe Seite 53).
- PAMUsers-Gruppenberechtigungen (siehe Seite 54).

Das Bearbeiten der Standardrollen und das Erstellen anwenderspezifischer Rollen ist eine erweiterte Funktion.

PAMAdmins-Gruppenberechtigungen

Die CA EEM-Richtlinien, die CA Process Automation bereitstellt, gewähren der PAMAdmins-Anwendungsgruppe alle Berechtigungen. Weisen Sie diese Gruppe den Administratoren zu, die vollständigen Zugriff auf CA Process Automation benötigen. Die Gruppe "PAMAdmins" stellt folgenden Zugriff auf Registerkartenebene bereit:

Startseite

Administratoren in der Gruppe "PAMAdmins" haben vollständigen Zugriff auf die Registerkarte "Startseite". Vollständiger Zugriff besteht aus der Berechtigung, sich bei CA Process Automation anzumelden und die Registerkarte "Startseite" zu verwenden (PAM40-Anwenderanmeldungsrichtlinie).

Bibliothek

Administratoren in der Gruppe "PAMAdmins" haben vollständigen Zugriff auf die Registerkarte "Bibliothek", die aus folgenden Berechtigungen besteht:

- Anzeigen der Registerkarte "Bibliothek" (PAM40-LibraryBrowser-Richtlinie).
- Steuern des Bibliotheksordners und der Ordnerinhalte (Environment_Library_Admin-Berechtigung in der PAM40-Umgebungsrichtlinie).
- Konfigurieren der Variablen, die zu einer Gruppe von anwenderspezifischen Operatoren gehören und Veröffentlichen der Gruppenkonfiguration im Auswahlmenü "Konfigurationsbrowser" auf der Registerkarte "Module" (PAM40-Gruppenkonfigurationsrichtlinie).

Designer

Administratoren in der Gruppe "PAMAdmins" haben vollständigen Zugriff auf die Registerkarte "Designer", die aus folgenden Berechtigungen besteht:

- Zeigen Sie die Registerkarte "Designer" an (Designer-Richtlinie).
- Volle Rechte auf der Registerkarte "Designer" (Environment_Library_Admin-Berechtigungen in der PAM40-Umgebungsrichtlinie).

Vorgänge

Administratoren in der Gruppe "PAMAdmins" haben vollständigen Zugriff auf die Registerkarte "Vorgänge", die aus folgenden Berechtigungen besteht:

- Anzeigen aller Auswahlmenüs auf der Registerkarte "Vorgänge" (PAM40-Vorgangsrichtlinie).
- Volle Berechtigungen (Environment_Library_Admin-Berechtigungen in der PAM40-Umgebungsrichtlinie).

Konfiguration

Administratoren in der Gruppe "PAMAdmins" haben vollständigen Zugriff auf die Registerkarte "Konfiguration", die aus folgenden Berechtigungen besteht:

- Anzeigen aller Auswahlmenüs im Auswahlmenü "Konfigurationsbrowser" (PAM40-Konfigurationsrichtlinie).
- Konfigurieren auf Domänenebene oder Ausführen einer Aktion, für die es erforderlich ist, die Domäne zu sperren (PAM40-Domänenrichtlinie).
- Konfigurieren auf Umgebungsebene oder Ausführen einer Aktion, für die es erforderlich ist, die Umgebung zu sperren (Environment_Config_Admin-Rechte in der PAM40-Umgebungsrichtlinie).
- Installieren der Agenten oder Koordinationsrechner (PAM40-Konfigurationsrichtlinie).
- Verwalten Sie Anwenderressourcen (PAM40-Konfigurationsrichtlinie).

Berichte

Administratoren in der Gruppe "PAMAdmins" haben vollständigen Zugriff auf die Registerkarte "Berichte". Vollständiger Zugriff besteht aus den Berechtigungen, um die Registerkarte "Berichte" anzuzeigen, Berichte zu generieren und neue Berichte hinzuzufügen (PAM40-Berichtsrichtlinie).

Designer-Gruppenberechtigungen

Standardmäßig enthält die Anwendungsgruppe "Designer" Berechtigungen, die Anwender in der Designumgebung benötigen. Die Gruppe "Designer" stellt folgenden Zugriff auf Registerkartenebene bereit:

Startseite

Anwender in der Gruppe "Designer" können sich bei CA Process Automation anmelden und die Registerkarte "Startseite" verwenden (PAM40-Anwenderanmeldungsrichtlinie).

Bibliothek

Anwender in der Gruppe "Designer" haben folgenden Zugriff auf die Registerkarte "Bibliothek":

- Anzeigen der Registerkarte "Bibliothek" (PAM40-LibraryBrowser-Richtlinie).
- Lesezugriff für Registerkarte "Bibliothek", einschließlich Berechtigung, um Automatisierungsobjekte anzuzeigen, zu exportieren und zu suchen (PAM40-Umgebungsrichtlinie).
- Steuern (Anzeigen, Navigieren, Bearbeiten, Löschen, Erstellen) von Ordnern auf der Registerkarte "Bibliothek" und Steuern aller Automatisierungsobjekte in den jeweiligen Editoren (PAM40-Objektrichtlinie).

Designer

Anwender in der Gruppe "Designer" haben folgenden Zugriff auf die Registerkarte "Designer":

- Zeigen Sie die Registerkarte "Designer" an (PAM40-Designerrichtlinie).
- Entwerfen von automatischen Prozessen und Steuern (Anzeigen, Navigieren, Bearbeiten, Löschen und Erstellen) aller Automatisierungsobjekte in den jeweiligen Editoren. Die Registerkarte "Designer" ist der Prozessautomatisierungs-Objekteditor (PAM40-Objektrichtlinie).

Vorgänge

Anwender in der Gruppe "Designer" haben folgenden Zugriff auf die Registerkarte "Vorgänge":

- Anzeigen aller Auswahlmenüs auf der Registerkarte "Vorgänge" (PAM40-Vorgangsrichtlinie).
- Steuern der Ablaufpläne, die auf der Registerkarte "Vorgänge" angezeigt werden (PAM40-Ablaufplanrichtlinie).
- Untersuchen und Ändern des Datensatzautomatisierungsobjekts (PAM40-Datensatzrichtlinie).
- Steuern, Starten und Überwachen des Prozessautomatisierungsobjekts (PAM40-Prozessrichtlinie).
- Steuern des Ressourcenautomatisierungsobjekts (PAM40-Ressourcenrichtlinie).
- Starten der Startauftragsformularrichtlinie und Entfernen aus der Warteschlange (PAM40-Startauftragsformular-Richtlinie).
- Anzeigen der Release-Version von importierten vordefinierten Inhalten, und Anzeigen der Objekte, die das Paket enthält.

Konfiguration

Anwender in der Gruppe "Designer" können die Registerkarten für einen Knoten anzeigen, den sie im Auswahlmenü "Konfigurationsbrowser" auswählen (PAM40-Konfigurationsrichtlinie).

Berichte

Anwender in der Gruppe "Designer" können die Registerkarte "Berichte" anzeigen, Berichte generieren und Berichte hinzufügen. Die Gruppe "Designer" basiert auf der Gruppe "PAMUsers", die auch diese Berechtigungen hat.

Produktionsanwender-Gruppenberechtigungen

Standardmäßig enthält die Anwendungsgruppe "Produktionsanwender" Berechtigungen, die Anwender in der Produktionsumgebung benötigen. Die Gruppe "Produktionsanwender" stellt folgenden Zugriff auf Registerkartenebene bereit:

Startseite

Anwender, die der Gruppe "Produktionsanwender" zugewiesen sind, haben Zugriff, um sich bei CA Process Automation anzumelden und die Registerkarte "Startseite" zu verwenden (PAM40-Anwenderanmeldungsrichtlinie).

Bibliothek

Anwender in der Gruppe "Produktionsanwender" haben folgenden Zugriff auf die Registerkarte "Bibliothek":

- Anzeigen der Registerkarte "Bibliothek" (PAM40-LibraryBrowser-Richtlinie).
- Lesezugriff auf die Registerkarte "Bibliothek" (PAM40-Umgebungsrichtlinie, die Voraussetzung der PAM40-Objektrichtlinie ist).
- Navigieren Sie durch die Ordnerstruktur auf der Registerkarte "Bibliothek", und zeigen Sie Automatisierungsobjekte an, die in den einzelnen Ordnern aufgelistet sind (PAM40-Objektrichtlinie).

Vorgänge

Anwender in der Gruppe "Produktionsanwender" haben folgenden Zugriff auf die Registerkarte "Vorgänge":

- Anzeigen aller Auswahlmenüs auf der Registerkarte "Vorgänge" (PAM40-Vorgangsrichtlinie).
- Steuern der Ablaufpläne, die auf der Registerkarte "Vorgänge" angezeigt werden (PAM40-Ablaufplanrichtlinie).
- Untersuchen von Datensätzen, die auf der Registerkarte "Vorgänge" im Auswahlmenü "Datensatz" angezeigt wird (PAM40-Datensatzrichtlinie).
- Überwachen oder Starten eines Prozesses, der auf der Registerkarte "Vorgänge" angezeigt wird (PAM40-Prozessrichtlinie).
- Starten des Startauftragsformulars, das auf der Registerkarte "Vorgänge" angezeigt wird, und Entfernen des Startauftragsformulars aus der Warteschlange (PAM40-Startauftragsformular-Richtlinie).
- Anzeigen der Release-Version von importierten vordefinierten Inhalten, und Anzeigen der Objekte, die das Paket enthält.

Konfiguration

Anwender in der Gruppe "Produktionsanwender" können die Registerkarten für einen Knoten anzeigen, den sie im Auswahlmenü "Konfigurationsbrowser" auswählen (PAM40-Konfigurationsrichtlinie).

Berichte

Anwender in der Gruppe "Produktionsanwender" können die Registerkarte "Berichte" anzeigen, Berichte generieren und Berichte hinzufügen (PAM40-Berichtsrichtlinie).

PAMUsers-Gruppenberechtigungen

Standardmäßig enthält die Anwendungsgruppe "PAMUsers" grundlegende Berechtigungen. Sie können diese Gruppe verwenden, um die anwenderspezifischen Gruppen zu ergänzen, die Sie für den präzise abgestimmten, rollenbasierten Zugriff erstellen. Die Gruppe "PAMUsers" stellt folgenden Zugriff auf Registerkartenebene bereit:

Startseite

Anwender in der Gruppe "PAMUsers" können sich bei CA Process Automation anmelden und die Registerkarte "Startseite" verwenden (PAM40-Anwenderanmeldungsrichtlinie).

Bibliothek

Anwender in der Gruppe "PAMUsers" haben folgenden Zugriff auf die Registerkarte "Bibliothek":

- Anzeigen der Registerkarte "Bibliothek" (PAM40-LibraryBrowser-Richtlinie).
- Lesezugriff auf die Registerkarte "Bibliothek" (PAM40-Umgebungsrichtlinie).

Vorgänge

Anwender in der Gruppe "PAMUsers" können die Registerkarte "Vorgänge" anzeigen (PAM40-Betriebsrichtlinie).

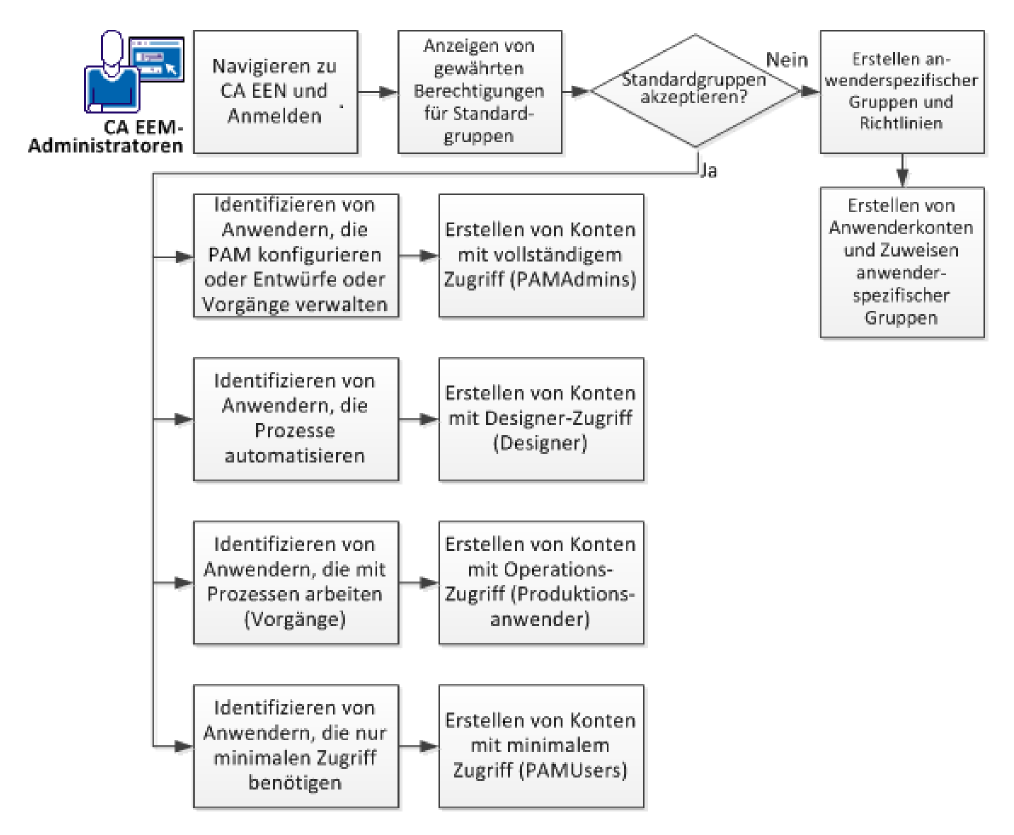
Berichte

Anwender in der Gruppe "PAMUsers" können die Registerkarte "Berichte" anzeigen, Berichte generieren und Berichte hinzufügen (PAM40-Berichtsrichtlinie).

Erstellen von Anwenderkonten mit Standardrollen

Wenn das Installationsprogramm CA EEM für die Verwendung eines internen Anwenderspeichers konfiguriert, erstellt der CA EEM-Administrator ein Anwenderkonto für jeden CA Process Automation-Anwender. Diese Anwenderkonten werden verwendet, um Anwender zu authentifizieren, wenn sie sich bei CA Process Automation anmelden. Um diese Anwender für den Zugriff auf Funktionen zu autorisieren, die für ihre Rollen erforderlich sind, weist der CA EEM-Administrator jedem Anwenderkonto die entsprechende Standardgruppe zu.

Die folgende Abbildung zeigt, wie Sie Anwenderkonten mit Standardrollen erstellen können. Die gestrichelten Linien zeigen die Aufgaben an, die Sie außerhalb von CA Process Automation ausführen.



Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Überprüfen Sie Berechtigungen für Standardgruppen.
   - PAMAdmins-Gruppenberechtigungen (siehe Seite 50)
   - Designer-Gruppenberechtigungen (siehe Seite 51)

- Produktionsanwender-Gruppenberechtigungen (siehe Seite 53)
- PAMUsers-Gruppenberechtigungen (siehe Seite 54)

3. Erstellen von Anwenderkonten für Administratoren (siehe Seite 56).
4. Erstellen von Anwenderkonten für Designer (siehe Seite 57).
5. Erstellen Sie Anwenderkonten für Produktionsanwender (siehe Seite 58).
6. Hinzufügen neuer Anwender zu CA Process Automation (siehe Seite 60).

Erstellen von Anwenderkonten für Administratoren.

Administratoren benötigen umfassenden Zugriff auf alle CA Process Automation-Funktionen. Um diesen Zugriff zu gewähren, ordnen Sie die Administrator-Anwenderkonten zur Gruppe "PAMAdmins" zu.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte Identitäten verwalten.
3. Klicken Sie im Auswahlmenü "Anwender" auf das Symbol neben "Anwender".

   Die Seite Neuer Benutzer wird angezeigt.
4. Geben Sie im Feld "Anwendername" die Anwender-ID ein, die dem Anwenderkonto zugewiesen werden soll.

   Der Anwender gibt diesen Wert bei der Anmeldung im Feld "Anwendername" ein.
5. Klicken Sie auf Anwendungsbenutzerdetails hinzufügen.

   Der Bereich wird aktualisiert, um den Abschnitt Anwendungsgruppenmitgliedschaft anzuzeigen.
6. Wählen Sie in "Verfügbare Benutzergruppen" "PAMAdmins" aus, und klicken Sie auf das Symbol ">", um sie in "Ausgewählte Benutzergruppen" zu verschieben.
7. Geben Sie die globalen Anwenderdetails ein.

   a. Geben Sie den Namen in die Felder Vorname und Nachname ein.

      Die Titelleiste zeigt diese Werte an, wenn der Anwender sich bei CA Process Automation anmeldet.

   b. Füllen Sie die weiteren Felder im Bereich Allgemein aus.
8. (Optional) Wenn Sie CA Process Automation mit einem anderen CA Technologies-Produkt verwenden, das CA EEM verwendet, dann füllen Sie den Abschnitt "Globale Gruppenmitgliedschaft" aus.

9. Geben Sie temporäre Authentifizierungsinformationen für dieses Anwenderkonto an:
   a. Wählen Sie Kennwort bei nächster Anmeldung ändern aus.
   b. Geben Sie im Feld Neues Kennwort ein temporäres Kennwort ein.
   c. Geben Sie dasselbe temporäre Kennwort im Feld Kennwort bestätigen ein.
10. (Optional) Füllen Sie die verbleibenden Felder auf der Seite Neuer Benutzer aus.
11. Klicken Sie auf "Speichern", und klicken Sie anschließend auf "Schließen".
12. (Optional) Klicken Sie auf "Abmelden".

Erstellen von Anwenderkonten für Designer

Erstellen Sie ein Anwenderkonto für jeden Designer, der Zugriff auf Automatisierungsobjekte in CA Process Automation benötigt. Automatisierungsobjekte werden verwendet, um Prozesse zu automatisieren.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Klicken Sie auf "Neuer Anwender".

   Die Seite "Neuer Anwender" wird angezeigt.
4. Geben Sie die Anwender-ID an, die dem Anwenderkonto im Namensfeld zugewiesen werden soll.
5. Klicken Sie auf "Anwendungsanwenderdetails hinzufügen".
6. Wählen Sie in "Verfügbare Benutzergruppen" "Designer" aus, und klicken Sie auf das Symbol ">", um sie in "Ausgewählte Benutzergruppen" zu verschieben.
7. Geben Sie die globalen Anwenderdetails ein.
8. Geben Sie ein Kennwort ein und bestätigen Sie es.

   Anwender können ihr eigenes Kennwort in CA EEM ändern.
9. (Optional) Füllen Sie die verbleibenden Felder auf der Seite "Neuer Anwender" aus.
10. Klicken Sie auf "Speichern" und anschließend auf "Schließen".
11. Klicken Sie auf "Abmelden".

Erstellen von Anwenderkonten für Produktionsanwender

Erstellen Sie ein Anwenderkonto für jeden Produktionsanwender, der auf CA Process Automation zugreifen muss, um automatische Prozesse zu überwachen und mit ihnen zu interagieren.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Klicken Sie auf "Neuer Anwender".

   Die Seite "Neuer Anwender" wird angezeigt.
4. Geben Sie die Anwender-ID an, die dem Anwenderkonto im Namensfeld zugewiesen werden soll.
5. Klicken Sie auf "Anwendungsanwenderdetails hinzufügen".
6. Wählen Sie in "Verfügbare Benutzergruppen" "Produktionsanwender" aus, und klicken Sie auf das Symbol ">", um sie in "Ausgewählte Benutzergruppen" zu verschieben.
7. Geben Sie die globalen Anwenderdetails ein.
8. Geben Sie ein Kennwort ein und bestätigen Sie es.

   Anwender können ihr eigenes Kennwort in CA EEM ändern.
9. (Optional) Füllen Sie die verbleibenden Felder auf der Seite "Neuer Anwender" aus.
10. Klicken Sie auf "Speichern" und anschließend auf "Schließen".
11. Klicken Sie auf "Abmelden".

Erstellen von Anwenderkonten mit grundlegendem Zugriff

PAMUsers ist eine Standardgruppe, die die Verwendung der Registerkarte "Startseite" und der Registerkarte "Berichte" gewährt. Für die Registerkarte "Bibliothek" und die Registerkarte "Vorgänge" wird nur schreibgeschützter Zugriff gewährt. Ein Anwender, der nur über PAMUsers-Zugriff verfügt, kann sich mit dem Produkt vertraut machen, jedoch kann der Anwender keine Objekte erstellen oder konfigurieren.

Verwenden Sie diese Gruppe als Grundlage für anwenderspezifische Gruppen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte Identitäten verwalten.
3. Klicken Sie auf "Neuer Anwender".

4. Geben Sie die Anwender-ID an, die dem Anwenderkonto im Namensfeld zugewiesen werden soll.
5. Klicken Sie auf "Anwendungsanwenderdetails hinzufügen", und klicken Sie auf das Symbol ">", um "PAMUsers" in "Ausgewählte Benutzergruppen" zu verschieben.
6. Geben Sie die globalen Anwenderdetails ein.
7. Geben Sie ein Kennwort ein und bestätigen Sie es.

   Anwender können sich bei CA EEM mit ihren CA Process Automation-Anmeldeinformationen anmelden und ihr eigenes Kennwort ändern.
8. (Optional) Füllen Sie die verbleibenden Felder auf der Seite Neuer Benutzer aus.
9. Klicken Sie auf "Speichern", und klicken Sie auf "Schließen".
10. Klicken Sie auf "Abmelden".

Einführen neuer Anwender in CA Process Automation

Um neuen Anwendern dabei zu helfen, produktiv zu werden, geben Sie folgende Informationen an:

Zugriffsinformationen

- Die CA Process Automation-URL. Dies kann die URL des Domänen-Koordinationsrechners oder die URL zum Lastenausgleich für den Domänen-Koordinationsrechner sein. Optional können Sie das System nach der URL eines beliebigen spezifischen Koordinationsrechners durchsuchen.
- Anmeldeinformationen. Anwender melden sich mit dem Anwendernamen und Kennwort an, das in ihrem CA EEM-Anwenderkonto konfiguriert ist.
- Die CA EEM-URL. Anwender melden sich mit dem von Ihnen zugewiesenen Anwendernamen und Kennwort an und wählen anschließend ein neues Kennwort aus.

  Hinweis: Wenn CA EEM auf mindestens ein externes Microsoft Active Directory-Verzeichnis verweist, müssen sich Anwender nicht bei CA EEM anmelden. Kennwörter werden von AD verwaltet.

Zugriff auf Ressourcen, um eine schnelle Einarbeitung zu ermöglichen

- Empfehlen Sie den Anwendern, die CA Process Automation-Lernprogramme zu nutzen, die auf der Registerkarte "Startseite" zur Verfügung stehen.
- Zeigen Sie Anwendern, dass sie auf das Bookshelf zugreifen können, indem sie die Option "Bookshelf" über die Verknüpfung "HILFE" in der Symbolleiste auswählen. Vom Bookshelf können Anwender auf die Handbücher für ihre Rolle zugreifen.

  Die Handbücher für jede Anwendungsgruppe (Rolle) sind:

  PAMAdmins

  > *Versionshinweise*
  >
  > *Installationshandbuch*
  >
  > *Handbuch für Inhaltsadministratoren*
  >
  > *Benutzeroberflächen-Referenzhandbuch*

  Designer

  > *Handbuch für Inhaltsdesign*
  >
  > *Referenzhandbuch für Inhaltsdesign*
  >
  > *Webservice-API-Referenzhandbuch*
  >
  > *Produktionsanwenderhandbuch*
  >
  > *Benutzeroberflächen-Referenzhandbuch*

  Produktionsanwender

  > *Produktionsanwenderhandbuch*

Benutzeroberflächen-Referenzhandbuch

Aktualisieren von Anwenderkonten mit Standardrollen

Führen Sie ein Upgrade der Anwender durch, die vorher "PAMAdmins" (oder "ITPAMAdmins") zugewiesen haben, da die Gruppe für Designer oder Produktionsanwender die Sicherheit verbessern können. Wenn Sie ein Anwender sind, für den ein Upgrade durchgeführt wurde, weisen Sie gegebenenfalls folgende Standardgruppen zu Anwendern zu, die folgende Rollen ausführen:

- Designer
- Produktionsanwender

Hinweis: Wenn Sie vorher PAMUsers (oder ITPAMUsers) zu Anwenderkonten von einzelnen Anwendern zugewiesen haben, die mit "Aufgabenlisten", "Standardmäßige Prozessüberwachung" oder "Anwenderanfragen" gearbeitet haben, weisen Sie die Produktionsanwendergruppe zu diesen Konten neu zu.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Erweitern Sie das Auswahlmenü "Benutzer suchen", wählen Sie die Anwendungsbenutzer aus, geben Sie folgende Kriterien ein, und klicken Sie dann auf "Los".
   - Attribut: Gruppenmitgliedschaft
   - Operator: LIKE
   - Wert: PAMAdmins

   Die Liste der Anwenderkonten wird angezeigt, die gegenwärtig der Gruppe "PAMAdmins" zugewiesen ist.
4. Klicken Sie auf den Namen eines Anwenders, der ein Designer oder ein Produktionsanwender ist.

   Das ausgewählte Anwenderkonto wird geöffnet.
5. Wählen Sie "PAMAdmins" aus "Ausgewählte Benutzergruppen" aus, und klicken Sie auf den linken Pfeil.

   Die ausgewählte Gruppe wird aus "Ausgewählte Benutzergruppen" entfernt.

6. Wählen Sie in "Verfügbare Benutzergruppen" eine anwendbare Gruppe aus, und klicken Sie auf das Symbol ">", um sie in "Ausgewählte Benutzergruppen" zu verschieben.
   - Wählen Sie für Inhaltsdesigner "Designer" aus.
   - Wählen Sie für Produktionsanwender "Produktionsanwender" aus.
7. Klicken Sie auf "Speichern" und anschließend auf "Schließen".
8. Klicken Sie auf "Abmelden".

Verwalten der Zugriffe für referenzierte Anwenderkonten

Wenn Sie während der CA EEM-Installation auf einen externen Anwenderspeicher verweisen, werden globale Gruppen und Anwenderkonten automatisch in CA EEM geladen. CA Process Automation ermöglicht das Laden von bis 10000 Konten mit einem konfigurierbaren Parameter, der die CA EEM-Einstellung von 2000 erweitert. Informationen zum Anpassen dieser Einstellung finden Sie unter Festlegen der maximalen Anzahl von CA EEM-Anwendern oder -Gruppen (siehe Seite 64).

Die Anwenderkonten von einem referenzierten externen Anwenderspeicher werden als schreibgeschützte Datensätze geladen. Wenn ein neuer Anwender ein Konto benötigt, erstellen Sie es im externen Anwenderspeicher. Der neue Datensatz wird automatisch geladen. Sie können Zugriff auf CA Process Automation entweder auf der globalen Gruppenebene oder auf der globalen Anwenderebene bereitstellen.

Sie konfigurieren CA EEM, um den Zugriff auf CA Process Automation und die zugehörigen Komponenten zu ermöglichen, der referenzierte Anwenderspeicher verwaltet jedoch die Authentifizierung. Um sich bei CA Process Automation anzumelden, verwenden die globalen Anwender mit Anmeldungszugriff den Anwendernamen und das Kennwort (oder den Prinzipalnamen und das Kennwort) im referenzierten Anwenderspeicher.

Hinweis: Sie können CA EEM nicht verwenden, um Anwenderdatensätze zu aktualisieren, die in einem externen Anwenderspeicher gespeichert sind.

Gehen Sie wie folgt vor, um den Zugriff für Anwender mit Konten, die in einem externen Anwenderspeicher gespeichert werden, zu verwalten.

- Fügen Sie jedem globalen Anwenderkonto eine Anwendungsgruppe hinzu.

  Suchen Sie anhand des Namens nach jedem globalen Anwender. Weisen Sie dem globalen Anwenderkonto eine der Standardanwendungsgruppen (PAMAdmins, Designer, Produktionsanwender oder PAMUsers) oder eine anwenderspezifischen Gruppe zu. Sie können auch globale Gruppen erstellen und diesen ausgewählte globale Anwender hinzufügen.

  Wichtig! Geben Sie immer Kriterien ein, wenn Sie versuchen, die Anzeige aller Einträge in einem externen Anwenderspeicher zu vermeiden.

- Fügen Sie den CA Process Automation-Zugriffsrichtlinien eine globale Gruppe hinzu. Wählen Sie dann die zu gewährenden Aktionen aus.

  Fügen Sie den vordefinierten Richtlinien, die den Zugriff für alle Anwender in der Gruppe zuweisen, vor allem die globale Gruppe hinzu. Fügen Sie zum Beispiel der Anwenderanmeldungsrichtlinie "PAM40" die globale Gruppe hinzu, um allen globalen Anwendern in dieser globalen Gruppe den Anmeldezugriff auf CA Process Automation zu ermöglichen. Fügen Sie die Gruppe zur Designer-Richtlinie "PAM40" hinzu, um den Zugriff auf die Registerkarte "Designer" zu gewähren.

- Erstellen Sie eine aus ausgewählten globalen Anwendern oder globalen Gruppen bestehende dynamische Gruppe. Anwenderspezifische Anwendungsgruppen können einer dynamischen Gruppe hinzugefügt werden.

- Folgen Sie den Anweisungen in der Dokumentation, Integrieren von Active Directory mit CA EEM.

  Dieser Vorgang gewährt allen Anwendern in Ihrem AD vollen Zugriff auf CA Process Automation ohne eine Konfiguration in CA EEM. Die Implementierung ist hierbei zwar einfach, es mangelt dabei jedoch an der Sicherheit, die Sie bei rollenbasiertem Zugriff haben.

Wichtig! Bei LDAP-Servern von Drittanbietern konfigurieren Sie Folgendes unter "ou=system context level":

```
ou=Global Groups
```

Festlegen der maximalen Anzahl von CA EEM-Anwendern oder -Gruppen

Stellen Sie vor der Integration eines umfangreichen referenzierten Anwenderspeichers fest, ob der Speicher mehr als 10.000 Anwender und Gruppen enthält. Der Standardwert von "eem.max.search.size" (10.000) ist der Grenzwert für die Anzahl der Anwender und Gruppen, die CA Embedded Entitlements Manager während der Übertragung akzeptieren kann. Der CA Process Automation-Standardwert (10.000) erweitert den CA EEM-Standardwert (2.000).

Erhöhen Sie den Wert "eem.max.search.size", falls die folgende Meldung angezeigt wird, wenn Sie nach verfügbaren Anwendern suchen, ohne Suchkriterien zu definieren:

```
Obergrenze für Suche überschritten.
```

Um den Standardgrenzwert in der Datei "OasisConfig.properties" zu überschreiben, legen Sie den folgenden Parameter auf einen neuen Wert fest:

```
eem.max.search.size = 10000
```

Wenn Sie ein umfangreiches referenziertes Verzeichnis integrieren, legen Sie einen Wert fest, der größer ist als 20.000.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich als ein Administrator am Server an, auf dem der Domänen-Koordinationsrechner installiert ist.
2. Wechseln Sie zum folgenden Ordner:

   Installationsverzeichnis/server/c2o/.config

   Installationsverzeichnis

   Bezieht sich auf den Pfad, wo der Domänen-Koordinationsrechner installiert ist.
3. Öffnen Sie "OasisConfig.properties" mit einem Texteditor.
4. Verwenden Sie "Suchen", um den Parameter "eem.max.search.size" zu finden.
5. Ändern Sie den Wert von 10000 in einen entsprechenden Wert.
6. Speichern Sie die Datei, und schließen Sie den Texteditor.
7. Starten Sie den Koordinationsrechner neu:
   a. Stoppen Sie den Koordinationsrechner (siehe Seite 206).
   b. Starten Sie den Koordinationsrechner (siehe Seite 207).

Suchen nach Identitäten, die mit spezifischen Kriterien übereinstimmen

Wenn Sie auf einen großen externen Anwenderspeicher verweisen, geben Sie Suchkriterien an. Die Suchkriterien beschränken die zurückgegebenen globalen Anwenderkonto-Datensätze auf die benötigte oder auf eine entsprechende Teilmenge. Geben Sie einen **Vornamen wie z. B. "John"** an, um die Namen aller Anwender mit dem Vornamen "John" abzurufen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf Identitäten verwalten.
3. Wählen Sie im Bereich Benutzer suchen Globale Benutzer aus.
4. Überprüfen Sie die Drop-down-Liste "Attribute", und überprüfen Sie, ob die Anwender, nach denen Sie suchen, ein aufgelistetes Attribut als Wert haben.
   - Wenn ja, wählen Sie ein oder mehrere anwendbare Attribute aus. Wählen Sie zum Beispiel "Vorname" und "Nachname" aus.
   - Wählen Sie anderenfalls die Ellipse (...) aus, und geben Sie den Namen des Attributs ein, nach dem Sie suchen möchten.
5. Wählen Sie den Operator für den Ausdruck aus, und geben Sie einen Wert für das Attribut ein, das für die Zielanwenderkonten gilt. Der Wert kann ein Teilwert sein. Geben Sie zum Beispiel "s*" ein, um nach allen Datensätzen zu suchen, bei denen der Wert des ausgewählten Attributs mit dem Buchstaben "s" anfängt.

   Wichtig! Geben Sie bei der Suche immer Kriterien ein, um die Dauer der Abfrage von Einträgen aus einem externen Anwenderspeicher zu reduzieren.
6. Klicken Sie auf Los.

   Die Namen der globalen Anwender, die mit Ihren Auswahlkriterien übereinstimmen, werden im Bereich "Anwender" angezeigt. Die Namen werden im Format "Nachnamen, Vorname" angezeigt.

Beispiel: Ein Einzelanwender in zwei referenzierten Active Directorys

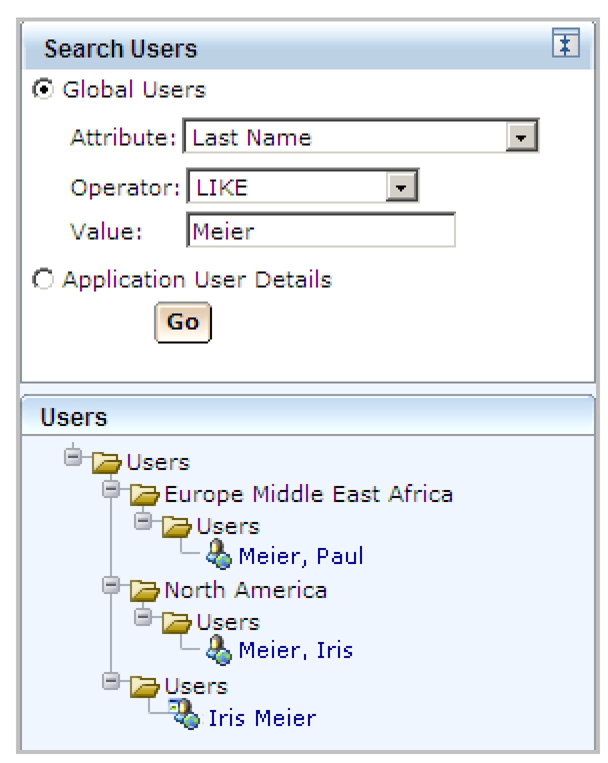
Annahmen:

- Vor dem Upgrade von CA Process Automation hat CA EEM auf ein externes Verzeichnis, ein Microsoft Active Directory, verwiesen. Die CA EEM-Version war r8.4
- Später, aber noch vor dem Upgrade von CA Process Automation, wurde ein CA EEM-Upgrade von r8.4 auf r12.51 durchgeführt. Die CA Process Automation-Anwender (d. h. referenzierte AD-Anwender, die einer Anwendungsgruppe zugewiesen sind), werden nach dem CA EEM-Upgrade in der Gruppenzuordnung beibehalten. Die globalen Anwender, die der Gruppe "Designer", die die Automatisierungsobjekte besitzen, zugewiesen sind, behalten den Objekteigentümer.
- Während des CA Process Automation-Upgrades auf r4.2 referenziert das Installationsprogramm mehrere ADs, eine Funktion, die ab CA EEM r12.5 unterstützt wird.
- Der CA EEM-Administrator muss jetzt eine Anwendungs-Anwendergruppe zu ausgewählten globalen Anwendern aus den zusätzlichen ADs zuweisen. Der Administrator weist auch Anwendungsgruppen zu CA Process Automation-Anwendern aus dem ursprünglichen AD erneut zu.
- Der CA EEM-Administrator gibt Suchkriterien für einen Anwender in einer der neu referenzierten AD-Domänen ein. Dieser Anwender ist in zwei Domänen, in der vorhandenen Domäne und in einer neuen Domäne. Obwohl jeder Anwender normalerweise in einer Domäne ist, ist es möglich, dass Anwender in mehr als einer AD-Domäne sind. In diesem Fall werden die zwei Anwenderkonten als verschiedene Anwender betrachtet, auch wenn sie sich möglicherweise auf den gleichen Einzelanwender beziehen.

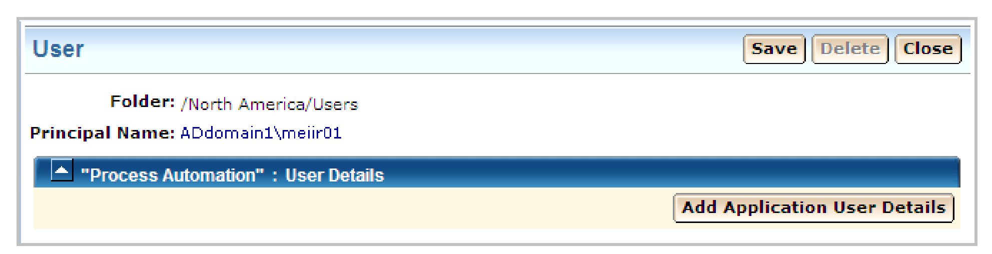
Der folgende Vorgang zeigt, wie dieses Beispiel in den CA EEM-Suchergebnissen und in den entsprechenden Anwenderdatensätzen angezeigt wird.

Gehen Sie folgendermaßen vor:

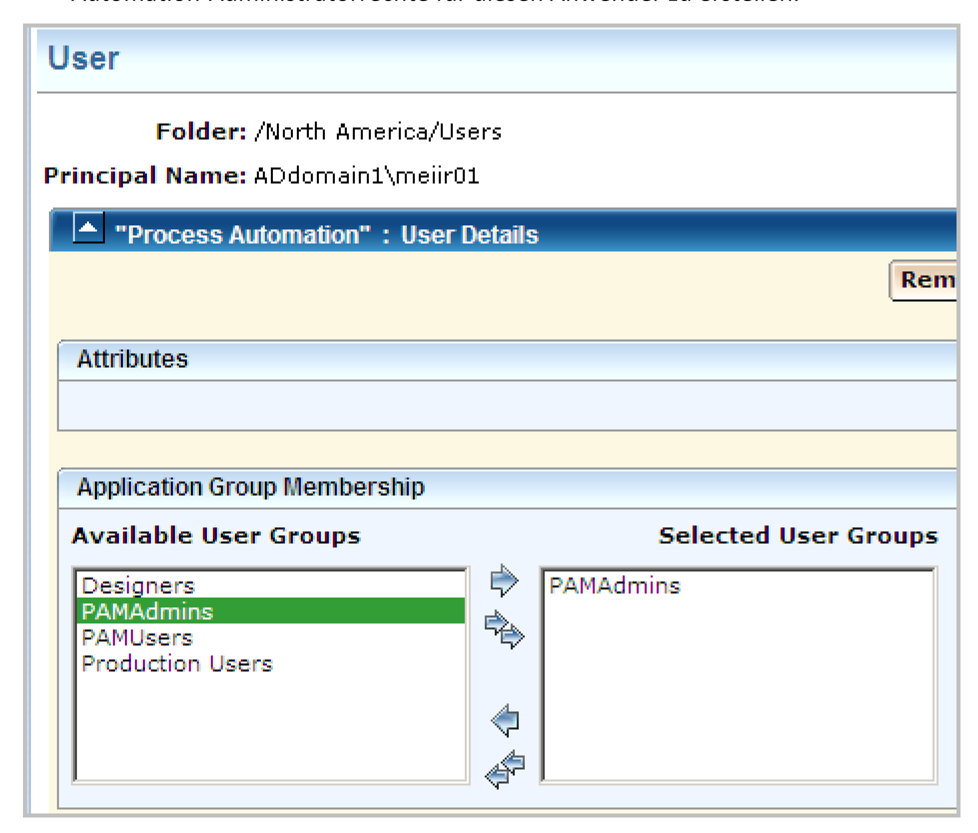
1. Melden Sie sich als CA EEM-Administrator bei CA EEM an.
2. Klicken Sie auf Identitäten verwalten. Geben Sie Suchkriterien für globale Anwender ein. Die Beispielsuche ist für alle AD-Anwender mit dem Nachnamen "Meier".



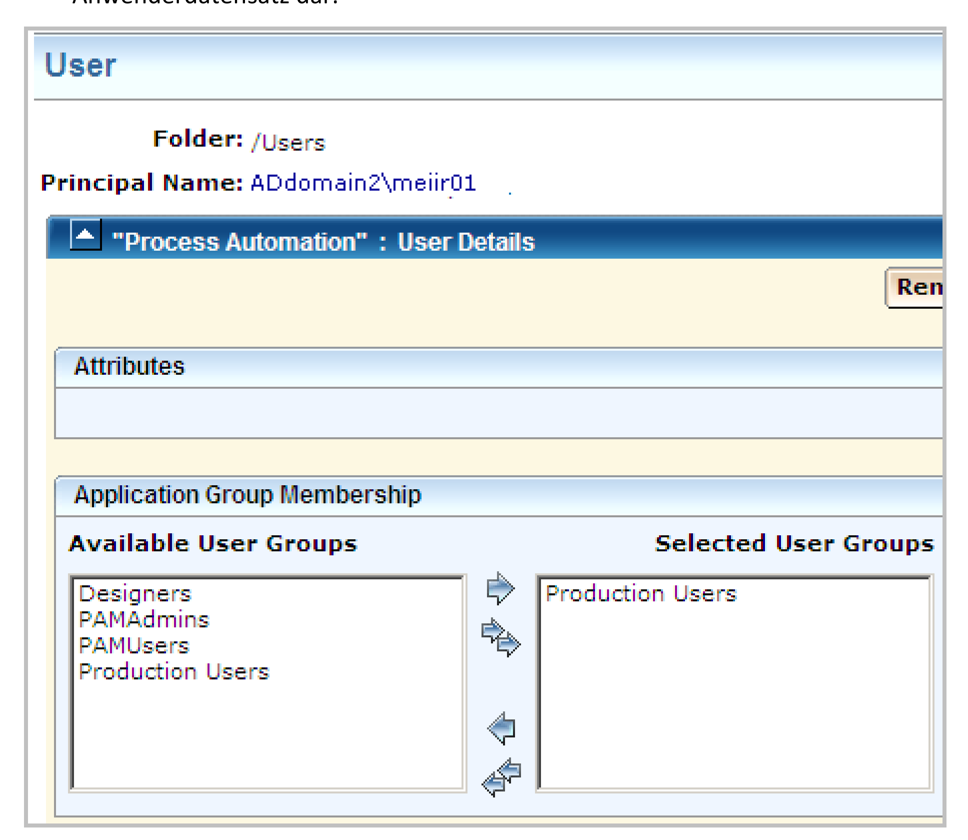
2. Wählen Sie einen der angezeigten globalen Anwender aus, wie z. B. "Meier, Iris". Der Bereich des Anwenderkontos wird geöffnet. Dieser Bereich stellt den Datensatz aus der neu referenzierten AD-Domäne dar. Klicken Sie auf Anwendungsbenutzerdetails hinzufügen.



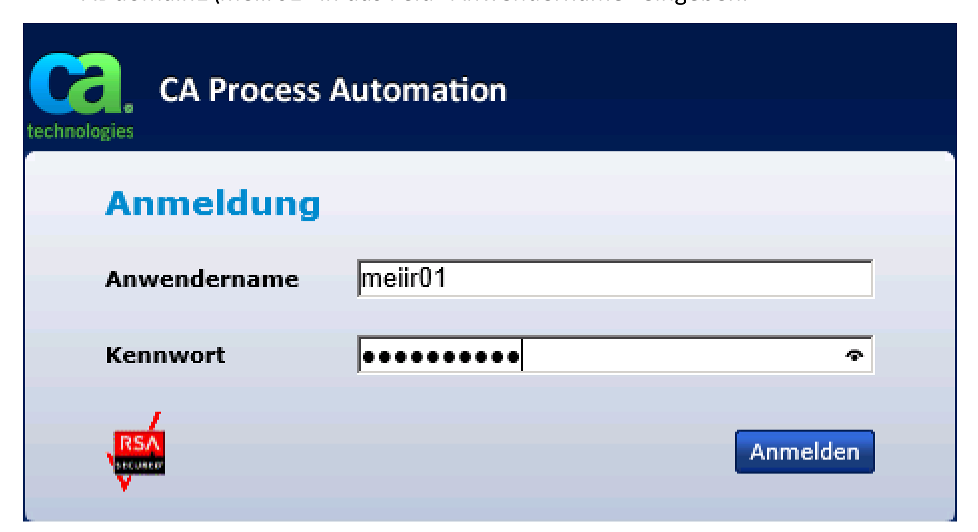
3. Wählen Sie die PAMAdmins-Anwendergruppe aus, um CA Process Automation-Administratorrechte für diesen Anwender zu erstellen.



4. Wählen Sie den anderen "Globaler Benutzer"-Eintrag aus den Suchergebnissen aus. Beachten Sie, dass dieser Eintrag "ADdomain2" und nicht "ADdomain1" anzeigt und über Produktionsanwender-Berechtigungen verfügt. Dies stellt den vorhandenen Anwenderdatensatz dar.



5. Der Anwender, der ursprünglich in der AD-Domäne referenziert wurde, kann sich bei CA Process Automation mit dem uneingeschränkten Anwendernamen anmelden, wenn diese Domäne als Standarddomäne festgelegt ist. (Alle Anwender von den zusätzlichen Domänen müssen bei der Anmeldung ihren Prinzipalnamen als Anwendernamen eingeben.) In diesem Beispiel führt die Eingabe des uneingeschränkten Anwendernamens dazu, dass der Anwender mit Produktionsanwender-Berechtigungen angemeldet wird. Um PAMAdmins-Berechtigungen abzurufen, würde der Anwender "ADdomain1\meiir01" in das Feld "Anwendername" eingeben.



Informationen zu globalen Benutzern

Alle für CA EEM definierten Anwender sind globale Anwender. Globale Anwender können folgende Typen sein:

- Anwender, für die Sie globale Anwenderkonten erstellen, in denen Sie alle Details angeben, darunter die Zuweisung einer Anwendungsgruppe und die Angabe eines Kennworts.
- Anwender, die in CA EEM für die Verwendung mit einem anderen CA-Produkt definiert sind. Sie suchen nach solchen globalen Anwendern, und Sie ermöglichen den CA Process Automation-Zugriff, indem Sie jedem Anwender eine CA Process Automation-Anwendungsgruppe zuweisen. Solche globalen Anwender melden sich bei CA Process Automation mit den zuvor in CA EEM definierten Anmeldeinformationen an.
- Anwender, die in einem externen Anwenderspeicher definiert wurden, die Sie beim Installieren von CA EEM definiert haben. Sie suchen nach solchen globalen Anwendern, und Sie ermöglichen den CA Process Automation-Zugriff, indem Sie jedem Anwender eine CA Process Automation-Anwendungsgruppe zuweisen. Solche globalen Anwender melden sich bei CA Process Automation mit den im externen Anwenderspeicher definierten Anmeldeinformationen an.

  Hinweis: Anwender geben Anmeldeinformationen entweder als Prinzipalname (*Domänenname\Anwendername*) und Kennwort ein, oder sie geben ihren Anwendernamen und ihr Kennwort ein. Der Prinzipalname wird *akzeptiert*, wenn CA EEM Microsoft Active Directory als externen Anwenderspeicher verwendet und wenn während der Installation auf mehrere Domänen verwiesen wird. Der Prinzipalname ist *erforderlich*, wenn die Quellen-AD-Domäne für den Anwender nicht die Standarddomäne ist.

Wenn Sie den internen Anwenderspeicher von CA EEM verwenden, erstellen Sie globale Anwender, und Sie weisen Anwendungsgruppen zu. Wenn Sie auf einen externen Anwenderspeicher verweisen, dann rufen Sie globale Anwender ab, und Sie weisen Anwendungsgruppen zu.

Zuweisen einer Anwendungsgruppe zu einem globalen Anwender

Um einem Anwender rollenbasierten Zugriff zu gewähren, weisen Sie dem jeweiligen globalen Anwenderkonto eine Anwendungsgruppe zu.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Suchen Sie nach Identitäten, die mit den angegebenen Kriterien übereinstimmen (siehe Seite 65).
3. Wählen Sie den Zielanwendernamen unter "Anwender" aus.

   Das ausgewählte Anwenderkonto wird geöffnet.

4. Klicken Sie auf Anwendungsbenutzerdetails hinzufügen.

   Das Dialogfeld Anwendungsgruppenmitgliedschaft wird geöffnet.

5. Wählen Sie in Verfügbare Benutzergruppen eine PAMUsers-Gruppe aus, und klicken Sie dann auf den Pfeil nach rechts (>), um sie in Ausgewählte Benutzergruppen zu verschieben.

6. Klicken Sie auf "Speichern".

   Der globale Zielanwender kann sich jetzt bei CA Process Automation anmelden. Nach dem Authentifizierungsprozess kann der Anwender auf die Funktion zugreifen, die das Produkt allen Mitgliedern der zugewiesenen Anwendungsgruppe gewährt.

Informationen zu dynamischen Anwendergruppen

Eine *dynamische Anwendergruppe* besteht aus globalen Anwendern, die ein oder mehrere Attribute gemeinsam nutzen. Sie wird über eine spezifische Richtlinie für dynamische Anwendergruppen erstellt. Der Ressourcenname ist der dynamische Anwendergruppenname, und die Mitgliedschaft basiert auf Filtern, die auf Anwender- und Gruppenattributen konfiguriert ist.

Sie können eine dynamische Anwendergruppe erstellen, die aus Anwendern, Anwendungsgruppen, globalen Gruppen oder dynamischen Gruppen besteht. Zum Beispiel können Sie eine dynamische Anwendergruppe aus globalen Gruppen oder Anwendungsgruppen basierend auf Name, Beschreibung oder Gruppenmitgliedschaft erstellen. Oder Sie können eine dynamische Anwendergruppe aus Anwendern mit unterschiedlichen Rollen basierend auf einem allgemeinen Attribut im globalen Anwenderprofil erstellen. Zum Beispiel:

- Berufsbezeichnung
- Abteilung oder Büro
- Stadt, Bundesland oder Land

Der EiamAdmin-Anwender kann dynamische Anwendergruppen-Richtlinien erstellen.

Erstellen einer dynamischen Anwendergruppen-Richtlinie

Sie können eine dynamische Anwendergruppen-Richtlinie erstellen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf Zugriffsrichtlinien verwalten und anschließend links von Richtlinien f. dynam. Benutzergruppen auf Neue Richtlinie für dynamische Gruppen.

3. Geben Sie für "Name" einen Gruppennamen ein, die eine allgemeine Eigenschaft der Gruppe von Anwendern identifiziert. Optional können Sie eine Beschreibung eingeben.
4. Wählen Sie einen Richtlinientyp aus. Der Standard lautet Zugriffsrichtlinie.
5. Wählen Sie folgendermaßen Identitäten aus:
    a. Wählen Sie für "Typ" einen der folgenden Werte aus, und klicken Sie dann auf "Identitäten suchen".
        - Anwender
        - Anwendungsgruppe
        - Globale Gruppe
        - Dynamische Gruppe
    b. Geben Sie unter "Attribut", "Operator" und "Wert" den Ausdruck ein, der die Kriterien für die Mitgliedschaft in dieser Gruppe festlegt, und klicken Sie auf "Suchen".

        Beispiel:

        Wählen Sie "Anwender" aus, geben Sie eine Berufsbezeichnung wie "**Manager**" ein, und klicken Sie auf "Suchen". Der Prozess gibt alle Anwender mit der Berufsbezeichnung "Manager" zurück.
    c. Wählen Sie aus den Suchergebnissen die Anwender aus, die als Mitglieder dieser dynamischen Gruppe hinzugefügt werden sollen. Um Ihre Auswahl in die Liste "Ausgewählte Identitäten" zu verschieben, klicken Sie auf den rechten Pfeil (>).
6. Wählen Sie für Aktionen gehören aus.
7. Geben Sie im Feld "Ressource hinzufügen" den Wert ein, den Sie im Feld "Name" angegeben haben, und klicken Sie dann auf "Hinzufügen".

    Der Prozess fügt die ausgewählten Identitäten der dynamischen Anwendergruppe hinzu, die Sie erstellt haben.
8. (Optional) Fügen Sie weitere Filter hinzu.
9. Klicken Sie auf "Speichern".

    Die Richtlinie, die Sie erstellt haben, wird angezeigt, wenn Sie auf den Link "Richtlinien f. dynam. Benutzergruppen" klicken.

Kapitel 4: Verwalten erweiterter CA EEM-Sicherheit

Sie können CA EEM verwenden, um präzise Zugriffsrichtlinien zu erstellen, um strenge Sicherheitsanforderungen zu erfüllen. Sie können anwenderdefinierte Richtlinien erstellen und Gruppen erstellen, die diese anwenderdefinierten Richtlinien verwenden, und Sie können Ihre anwenderspezifischen Gruppen den Anwenderkonten zuweisen. Oder Sie können Anwender direkt den anwenderdefinierten Richtlinien zuweisen. Sie können anwenderdefinierte Richtlinien erstellen, um den Zugriff auf einen oder mehrere angegebene Ordner, mit oder ohne Unterordner, zu beschränken. Zu den Zugriffsebenen gehören Anzeigen, Navigieren, Bearbeiten, Löschen und Erstellen, wobei Berechtigungen additiv sind. Sie können den Anwenderzugriff auf eine angegebene Umgebung beschränken. Sie können auch den Zugriff ändern, der für Standardgruppen definiert ist.

Anpassung ist erforderlich, um den Standardzugriff zu erweitern. Zum Beispiel wird eine Anpassung verwendet, um Administratoren Zugriff auf CA EEM zu gewähren, einen ähnlichen Zugriff zu erstellen, der durch die vorherige LDAP-Implementierung gewährt wird, und um den Zugriff auf Server einzuschränken, die vertrauliche Informationen oder kritische Business-Prozesse enthalten.

Der Abschnitt der Berechtigungsreferenz enthält Details, die alle Anpassungstypen unterstützen.

Dieses Kapitel enthält folgende Themen:

Gewähren von Zugriff auf CA EEM für Administratoren

CA EEM stellt Sicherheit für CA Process Automation bereit. CA EEM verwaltet die Anmeldeinformationen in Anwenderkonten, die Anwendern es ermöglichen, sich bei CA Process Automation anzumelden. CA EEM authentifiziert Anwender bei der Anmeldung und ermöglicht das Anmelden, wenn die Anwender-ID und das Kennwort in einem Anwenderkonto gefunden werden. Anwenderkonten werden Gruppen zugeordnet. CA EEM autorisiert Anwender bei der Anmeldung basierend auf ihren Gruppenzuweisungen.

"EiamAdmin" ist der vordefinierte Anwendername des CA EEM-Administrators. Der CA EEM-Administrator ist die Rolle, die Anwendern den Zugriff auf CA Process Automation zuweist. Während der Installation von CA Process Automation geben Sie ein Kennwort für den EiamAdmin-Anwender an. Nur Anwender, die das EiamAdmin-Kennwort kennen, können sich bei CA EEM anmelden. Wir empfehlen, dass Sie dieses Kennwort nur an wenige Vertrauenspersonen weitergeben.

Der EiamAdmin-Anwender kann eine Richtlinie definieren, die ausgewählten CA Process Automation-Administratoren das Recht gewährt, anwenderspezifische Gruppen, Richtlinien und Anwenderkonten zu erstellen. Dieser Zugriff ist ausreichend, jedoch ist er beschränkter als der Zugriff von EiamAdmin. Der Prozess umfasst Folgendes:

Administratoren Zugriff gewähren auf CA EEM

CA EEM-Administrator

Zu CA EEM Navigieren und sich anmelden

Anwender-konten für Administratoren erstellen

Ausgewählten Administratoren CA EEM-Zugriff gewähren

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Erstellen von Anwenderkonten für Administratoren (siehe Seite 56).
3. Gewähren von CA EEM-Zugriff zu ausgewählten Administratoren (siehe Seite 77).

Weitere Informationen:

Gewähren von CA EEM-Zugriff zu ausgewählten Administratoren. (siehe Seite 77)

Gewähren von CA EEM-Zugriff zu ausgewählten Administratoren.

CA EEM-Zugriff wird benötigt, um Anwenderkonten, Gruppen und Richtlinien zu verwalten. Standardmäßig müssen Sie das EiamAdmin-Kennwort kennen, um sich bei CA EEM mit der Anwendung, die für CA Process Automation eingerichtet ist, anzumelden. Normalerweise ist die Kenntnis des Kennworts sehr beschränkt, da der EiamAdmin-Anwender die volle Kontrolle über CA EEM hat. Allerdings kann der EiamAdmin-Anwender anderen Administratoren den CA EEM-Anmeldungszugriff gewähren, und er kann die Objekte angeben, die sie verwalten können. Folgender Vorgang zeigt, wie Sie ausgewählten Administratoren gewähren, Anwenderkonten, Gruppen und Richtlinien zu verwalten. Zum diesem Prozess gehören das Definieren einer neuen Gruppe, das Erstellen einer anwenderdefinierten Richtlinie für diese Gruppe, und das anschließende Zuweisen der Gruppe zu den Anwenderkonten.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Erstellen Sie EEMAdmins-Mitglieder, eine CA EEM-Administratorengruppe, die Anwenderkonten, anwenderspezifische Gruppen und anwenderdefinierte Richtlinien erstellen können.
    a. Klicken Sie auf die Registerkarte Identitäten verwalten.
    b. Klicken Sie auf Gruppen.
    c. Klicken Sie auf "Neue Anwendungsgruppe".
    d. Geben Sie einen Namen für die Gruppe ein (z. B. "EEMAdmins").
    e. (Optional) Fügen Sie eine Beschreibung hinzu.
    f. Klicken Sie auf "Speichern".

    Hinweis: Wählen Sie keine Anwendungsgruppe aus.

3. Erstellen Sie eine Richtlinie, die das Erstellen von Anwenderkonten, anwenderspezifischen Gruppen und anwenderdefinierten Richtlinien gewährt. Weisen Sie "EEMAdmins" als Identität für diese Richtlinie zu.

   a. Klicken Sie auf die Registerkarte Zugriffsrichtlinien verwalten.

   b. Klicken Sie auf die Richtlinien "Scoping".

   c. Klicken Sie auf die Verknüpfung zum Verwalten von Objekten.

   d. Klicken Sie auf "Speichern unter", und geben Sie einen Namen für diese Richtlinie ein (z. B. "Anwender und Richtlinien verwalten")

   e. Klicken Sie auf OK.

   f. Wählen Sie in der Liste "Ausgewählte Identitäten" "[User] EiamAdmin" und "[User] CERT-application-name" aus, und klicken Sie auf "Löschen".

   g. Klicken Sie auf "Identitäten suchen" als Gruppentyp, und klicken Sie dann auf "Suchen".

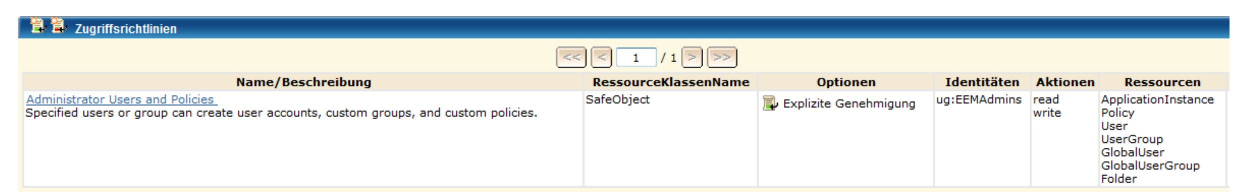
   h. Wählen Sie die neue Gruppe (EEMAdmins) aus, und klicken Sie auf den rechten Pfeil, um diese Anwendergruppe (ug) in "Ausgewählten Identitäten" zu verschieben.

   i. Wählen Sie alle Ressourcen mit *Ausnahme* von "Policy", "User", "UserGroup", "GlobalUser", "GlobalUserGroup" und "Folder" aus, und löschen Sie sie.

   j. Überprüfen Sie, dass die Aktionen "Lesen" und "Schreiben" ausgewählt sind.

   k. Klicken Sie auf "Speichern".

   Ihre Richtlinie ähnelt dem folgenden Beispiel:



Zugriffsrichtlinien

1 / 1

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Administrator Users and Policies Specified users or group can create user accounts, custom groups, and custom policies.	SafeObject	Explizite Genehmigung	ug:EEMAdmins	read write	ApplicationInstance Policy User UserGroup GlobalUser GlobalUserGroup Folder

4. Fügen Sie die Gruppe "EEMAdmins" den Anwenderkonten der ausgewählten Administratoren hinzu:
    a. Klicken Sie auf die Registerkarte Identitäten verwalten.
    b. Klicken Sie für "Benutzer suchen" auf "Anwendungsbenutzerdetails".
    c. Wählen Sie "Gruppenmitgliedschaft" als Attribut, "LIKE" als Operator und "PAMAdmins" als Wert aus.
    d. Klicken Sie auf Los.

       Die CA Process Automation-Administratoren werden aufgelistet.
    e. Klicken Sie auf den Namen eines Administrators.

       Das Anwenderkonto des ausgewählten Administrators wird geöffnet. "EEMAdmins" wird als verfügbare Anwendergruppe angezeigt.
    f. Klicken Sie auf den rechten Pfeil, um "EEMAdmins" in "Ausgewählte Benutzergruppen" zu verschieben.
    g. Klicken Sie auf "Speichern".
5. Wiederholen Sie Schritt 4 für jeden Administrator, dem Sie CA EEM-Rechte gewähren möchten.

Anpassung von Zugriffsrechten mit CA EEM-Richtlinien

Sie können den Anwenderzugriff auf Registerkarten und Auswahlmenüs von CA Process Automation anpassen und auf verschiedene Automatisierungsobjekte zugreifen. Um die Änderungen auf jeden in einer Standardgruppe auszuweiten, können Sie die Standardrichtlinien ändern.

Sie können den Anwenderzugriff auf angegebene Ordner beschränken. Zum Beispiel können Sie einen Ordner für jeden Designer erstellen und den Designerzugriff auf die eigenen Ordner und auf Ordner zur allgemeinen Verwendung beschränken.

Sie können den Zugriff auf eine angegebene Umgebung für angegebene Anwender beschränken. Zum Beispiel können Sie den Umgebungszugriff für Mitglieder der Gruppe "Produktionsanwender" beschränken, sodass sie nur auf die Produktionsumgebung zugreifen können. Die Mitglieder können dann nicht auf die Designumgebung zugreifen.

Sie können den Zugriff auf Kontaktpunkte beschränken, die Servern zuordnet sind, die vertrauliche Informationen enthalten oder kritische Business-Funktionen mit Richtlinien zur Kontaktpunktsicherheit ausführen.

Steuern von Zwischenspeichern von CA EEM-Aktualisierungen

CA Process Automation spiegelt die Änderungen nicht sofort wider, wenn Richtlinien, Anwendergruppen und Anwenderkonten in CA EEM geändert werden. CA Process Automation fragt CA EEM bei Autorisierunsgabfragen nicht immer direkt ab. CA EEM sendet einzelne Änderungen nicht in Echtzeit an CA Process Automation. Stattdessen verlässt sich CA Process Automation auf die folgenden Zwischenspeicher:

- Ein Zwischenspeicher auf CA EEM-Seite mit Änderungen an Richtlinien, Anwendergruppen und Anwenderkonten, die CA EEM an CA Process Automation sendet.

  Eine Sicherheitseinstellung auf der Registerkarte "Konfiguration" steuert die Aktualisierungsrate des Zwischenspeichers. Sie können die Einstellung auf Domänenebene oder für eine ausgewählte Umgebung aktualisieren.

- Ein sekundärer Zwischenspeicher auf CA Process Automation-Seite mit den Abfrageergebnissen, die CA EEM an CA Process Automation zurückgibt.

  Wenn die Sicherheitsfunktion Anwenderberechtigungen validiert, prüft sie als Erstes das Alter des sekundären Zwischenspeichers.

  - Wenn das Alter des Zwischenspeichers gleich oder niedriger als der konfigurierte Wert ist, verwendet die Sicherheitsfunktion die Berechtigungsdaten im Zwischenspeicher.
  - Wenn das Zwischenspeicheralter höher als der konfigurierte Wert ist, sendet die Sicherheitsfunktion eine Abfrage an CA EEM. Die Sicherheitsfunktion aktualisiert den sekundären Zwischenspeicher mit den Abfrageergebnissen und setzt das Zwischenspeicheralter auf 0 Sekunden zurück.

Wenn Sie anwenderspezifische Richtlinien mit einem Testanwender testen, können Sie die Ergebnisse anzeigen, sobald CA EEM Änderungen an CA Process Automation sendet. Um CA Process Automation häufiger zu aktualisieren, reduzieren Sie das Aktualisierungsintervall. Um die Produktleistung zu optimieren, wenn Sie die Tests beenden, erhöhen Sie das Aktualisierungsintervall des Zwischenspeichers.

Wenn Sie den folgenden Vorgang verwenden, um das Aktualisierungsintervall des Zwischenspeichers auf CA EEM-Seite zu ändern, erwägen Sie, nur in der Designumgebung eine hohe Aktualisierungsrate zu verwenden. Ändern Sie optional das maximale Alter des sekundären Zwischenspeichers auf dem Server, auf dem der Ziel-Koordinationsrechner für Tests gehostet wird.

Gehen Sie folgendermaßen vor:

1. Ändern Sie, wie oft CA Process Automation Aktualisierungen von CA EEM abruft. Legen Sie das standardmäßige Intervall auf Domänenebene fest.
   a. Klicken Sie auf die Registerkarte Konfiguration.

      Das Auswahlmenü Konfigurationsbrowser wird geöffnet, und Domäne ist ausgewählt. Die Registerkarte Sicherheit wird angezeigt.
   b. Klicken Sie auf Sperren.
   c. Bearbeiten Sie die Einstellung Aktualisierungsintervall der CA EEM-Cache-Aktualisierung (in Sekunden) nach Bedarf, basierend auf der Häufigkeit, mit der CA EEM aktualisiert wird.
      - Während Sie die Auswirkung von CA EEM-Änderungen testen, legen Sie das Aktualisierungsintervall auf **60** Sekunden fest.
      - Wenn Sie die Tests beenden, legen Sie das Aktualisierungsintervall auf **1800** Sekunden (den Standardwert) fest.
   d. Klicken Sie auf "Speichern".
   e. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".
   f. Starten Sie den Domänen-Koordinationsrechner erneut.
      - Stoppen Sie den Koordinationsrechner (siehe Seite 206).
      - Starten Sie den Koordinationsrechner (siehe Seite 207).

2. Ändern Sie die Frequenz, mit der CA EEM Autorisierungsänderungen für eine ausgewählte Umgebung an CA Process Automation sendet.

   a. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie die Option "Domäne" im Auswahlmenü "Konfigurationsbrowser".

   b. Wählen Sie die Zielumgebung aus, und klicken Sie auf Sperren.

   c. Bearbeiten Sie auf der Registerkarte Sicherheit die Einstellung Aktualisierungsintervall der CA EEM-Cache-Aktualisierung (in Sekunden) nach Bedarf, basierend darauf, ob Sie Anwenderautorisierungen aktiv testen.

      - Während Sie anwenderspezifische Anpassungen testen, legen Sie das Aktualisierungsintervall auf **60** Sekunden fest.

      - Wenn Sie die Tests beenden, legen Sie das Aktualisierungsintervall auf **1800** Sekunden (den Standardwert) fest.

   d. Klicken Sie auf "Speichern".

   e. Wählen Sie die Umgebung aus, und klicken Sie auf "Entsperren".

   f. Starten Sie die Koordinationsrechner in der Umgebung, die Sie aktualisiert haben, neu.

      - Stoppen Sie den Koordinationsrechner (siehe Seite 206).

      - Starten Sie den Koordinationsrechner (siehe Seite 207).

3. Ändern Sie das Höchstalter (in Sekunden) des sekundären Zwischenspeichers, der Anwenderberechtigungen enthält.

   Hinweis: Es ist normalerweise nicht notwendig, diesen internen Parameter zu ändern.

   a. Melden Sie sich bei dem Server an, auf dem der Ziel-Koordinationsrechner konfiguriert ist.

   b. Navigieren Sie zum folgenden Ordner oder Verzeichnis:

      `*Installationsverzeichnis*/server/c2o/.config/`

   c. Öffnen Sie die Datei "OasisConfig.properties".

   d. Fügen Sie den folgenden Parameter hinzu, wenn er nicht vorhanden ist:

      ```
      eem.cache.timeout
      ```

   e. Weisen Sie einen Wert zu (in Sekunden).

      Wenn Sie diesen Parameter auf 0 setzen, wird der Zwischenspeicher ausgeschaltet, sodass CA Process Automation Anwenderberechtigungen von CA EEM abfragt, wenn sie erforderlich sind. Das Produkt verwendet den Standardwert (30), wenn dieser Parameter in der Datei "OasisConfig.properties" nicht vorhanden ist.

      ```
      eem.cache.timeout=30
      ```

   f. Speichern Sie die Datei.

   g. Starten Sie den Koordinationsrechner-Service neu.

      ■ Stoppen Sie den Koordinationsrechner (siehe Seite 206).

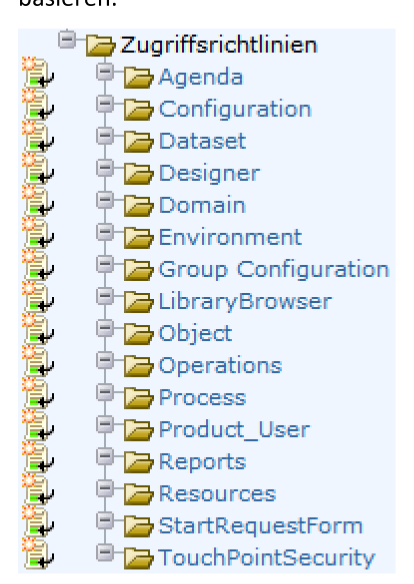
      ■ Starten Sie den Koordinationsrechner (siehe Seite 207).

Weitere Informationen:

Konfigurieren von CA EEM-Sicherheitseinstellungen für die Domäne (siehe Seite 150)

Standard-Ressourcenklassen und anwenderspezifische Richtlinien

CA Process Automation-Ressourcenklassen werden in CA EEM unter "Zugriffsrichtlinien" aufgelistet. Sie können eine ursprüngliche anwenderspezifische Richtlinie für eine Ressourcenklasse erstellen, oder Sie können sie auf eine vordefinierte Richtlinie basieren.



Die meisten CA EEM-Ressourcenklassen enthalten vordefinierte Richtlinien.

Sie können "Speichern unter" verwenden, um die vordefinierten Zugriffsrichtlinien mit einem neuen Namen zu speichern, und Sie können sie dann nach Bedarf anpassen. Wenn Sie eine anwenderspezifische Richtlinie erstellen, die auf eine vordefinierte Richtlinie basiert, können Sie folgende Ergebnisse erreichen:

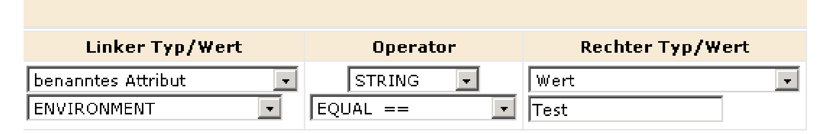
- Geben Sie der zugewiesenen Gruppe eine Berechtigung an, die die vordefinierte Richtlinie nicht gewährt. Durch die anwenderspezifische Richtlinie kann beispielsweise der Gruppe "Designer" Zugriff auf das Auswahlmenü "Installation" auf der Registerkarte "Konfiguration" gewährt werden, damit ihre Mitglieder Agenten installieren können.
- Entfernen Sie eine Berechtigung oder einen Zugriff, die bzw. der von einer vordefinierten Richtlinie gewährt wird. Zum Beispiel kann Ihre anwenderspezifische Richtlinie Zugriffsrechte auf die Gruppe "PAMUsers" auf der Registerkarte "Berichte" entfernen.
- Ersetzen Sie eine Standardgruppe (zum Beispiel "PAMAdmins") durch Gruppen, die die Produktrollen, die Ihr Standort definiert, besser darstellen. Zum Beispiel können Sie statt einer Administratorebene drei Administratorebenen haben. Weisen Sie "PAMAdmins" Ihrem Domänenadministrator zu, und erstellen Sie separate Administratorgruppen, die Inhalte verwalten und Konfigurationen für jede Umgebung ausführen.

  Hinweis: Weitere Informationen über das Erstellen von separaten Zugriffsrechten für Inhaltsadministratoren und Konfigurationsadministratoren finden Sie unter "Erstellen von Anwenderkonten mit anwenderspezifischen AD-Rollen (siehe Seite 119)".
- Fügen Sie einen oder mehrere Filter für einen präzise abgestimmten Zugriff hinzu. Zum Beispiel können Sie "UMGEBUNG" genau wie einen Umgebungsnamen als Filter angeben. Der Umgebungsfilter wird oft in anwenderspezifischen Richtlinien zur Kontaktpunktsicherheit verwendet.

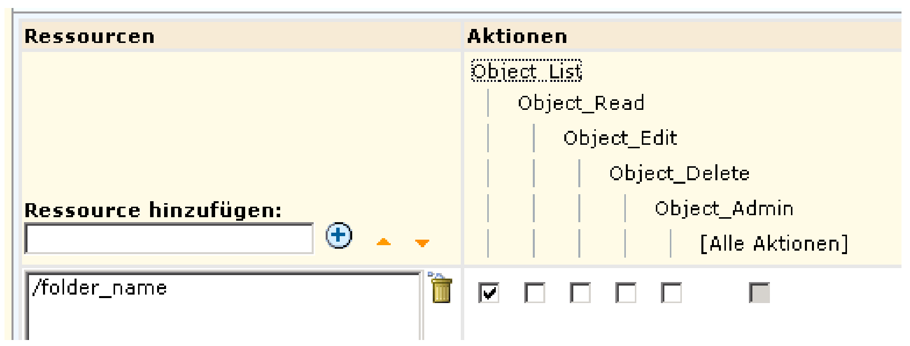
Beachten Sie die Prozess- und Startauftragsformular-Objekte bezüglich der Aufrufe der SOAP-Zugriffsebene durch Webservices. Wenn Sie eine Richtlinie mit der Ressourcenklasse "Prozess" erstellen, gewähren Sie den angegebenen Anwendern oder Gruppen die Rechte für "Process_Start (Start)" oder "Process_Control (Kontrolle)". Wenn der Anwender, der die Methode "Prozess ausführen" aufruft, über Berechtigungen zum Starten und Kontrollieren verfügt, wird die Methode erfolgreich ausgeführt. Wenn Sie eine Richtlinie mit der Ressourcenklasse "Startauftragsformular" erstellen, gewähren Sie angegebenen Anwendern oder den Gruppen "StartRequestForm_Start (Start)" oder "StartRequestForm_Dequeue (Aus Warteschlange entfernen)" Berechtigungen. Wenn der Anwender, der die Methode "Startauftragsformular ausführen" ausführt, über Berechtigungen zum Starten oder zum Entfernen aus der Warteschlange verfügt, wird die Methode erfolgreich ausgeführt. Wenn der Anwender, der die Methode ausführt, keine Ausführungsrechte auf dem Zielobjekt hat, schlägt die Methode fehl. Der SOAP-Operatordatensatz erfasst Fehlermeldungen der Methode.

Sie können eine anwenderspezifische CA EEM-Richtlinie erstellen, die den Zugriff von angegebenen Gruppen zu einem angegebenen Automatisierungsobjekt gewährt oder verweigert. Zum Beispiel:

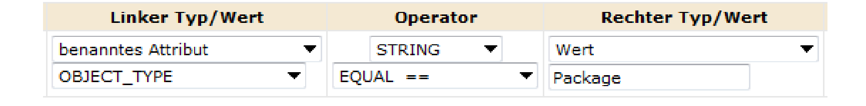
- Beschränken Sie den Zugriff auf eine angegebene Umgebung mit der Richtlinie "Agenda", "Datensatz", "System", "Prozess", "Ressourcen", "Startauftragsformular", "Kontaktpunktsicherheit". Fügen Sie einen Filter mit "Umgebung" als benanntem Attribut und dem Namen Ihrer Umgebung als Wert hinzu. Der Operator STRING ist EQUAL ==. Im folgenden Filterbeispiel ist "Test" der Name der Umgebung:



- Beschränken Sie Zugriff auf einen angegebenen Ordner oder angegebenes Objekt mit der Objekt-Richtlinie. Fügen Sie eine Ressource hinzu wie "/*folder_name*" oder "/*folder_name*/*object_name*". Im folgenden Beispiel steht "/folder_name" für den Namen des Ordners, in dem sich die Automatisierungsobjekte befinden.



Sie können auch eine anwenderspezifische Richtlinie für die Ressourcenklasse "Objekt" erstellen. Richtlinien für die Ressourcenklasse "Objekt" bieten einen Filter für die Angabe des Objekttyps, für den die Richtlinie gilt. Fügen Sie einen Filter mit "Objekttyp" als benanntem Attribut und einem Objekttyp als Wert hinzu. Der Operator STRING ist EQUAL ==. Im folgenden Filterbeispiel ist "Ressourcen" der Name des Objekttyps:



Andere gültige Werte lauten:

- Die Ressourcenklassen:
  - Agenda, die Ressourcenklasse für Ablaufplan.
  - Datensatz
  - Prozess
  - Ressourcen
  - Startauftragsformular
- Kalender
- Anwenderspezifisches Symbol
- Anwenderspezifischer Operator
- Ordner
- Interaktionsauftragsformular
- Prozessüberwachung

So passen Sie den Zugriff für eine Standardgruppe an

Sie können den standardmäßigen Zugriff folgendermaßen anpassen:

- Fügen Sie eine Aktion zu einer Standardgruppe hinzu.
- Widerrufen Sie eine Aktion von einer Standardgruppe.

Änderungen, die Sie in den Zuweisungen einer Standardgruppe vornehmen, wirken sich auf alle Anwender aus, die dieser Gruppe zugewiesen sind.

Der Vorgang für das Anpassen des Zugriffs für eine Standardgruppe:

1. Überprüfen Sie Berechtigungen für Standardgruppen (siehe Seite 48).
2. Identifizieren Sie eine Berechtigung, die an Ihrem Standort erforderlich ist und die einer Standardgruppe fehlt.
3. Bestimmen Sie die Aktion und die Richtlinie, die diesen Zugriff steuern.
   - Wenn die Berechtigung der Zugriff auf eine Registerkarte oder auf ein Auswahlmenü ist, finden Sie weitere Informationen unter Berechtigungen nach Registerkarten (siehe Seite 104).
   - Wenn sich die Berechtigung auf einem Automatisierungsobjekt befindet, finden Sie weitere Informationen unter Berechtigungen für Automatisierungsobjekte (siehe Seite 111).
4. Erstellen Sie eine Richtlinie, die auf einer vorhandenen Richtlinie basiert (siehe Seite 89), bei der die vorhandene Richtlinie eine vordefinierte Standardrichtlinie ist.
5. Gewähren oder widerrufen Sie eine Aktion für eine Standardgruppe (siehe Seite 89).

Erstellen einer anwenderdefinierten Richtlinie auf Basis einer vorhandenen Richtlinie

Sie können eine anwenderdefinierte Richtlinie erstellen, die auf einer Standardrichtlinie oder auf einer anderen anwenderdefinierten Richtlinie basiert.

CA Process Automation stellt eine Richtlinie für fast alle Ressourcenklassen bereit. Sie können Standardrichtlinien direkt ändern, da sie editierbar sind. Allerdings gibt es keine einfache Möglichkeit, sie wieder auf das Original zurückzusetzen. Sie können eine Vorgehensweise zur Erhaltung der vordefinierten Richtlinien einführen, sodass Sie eine Version mit dem Original vergleichen oder zur ursprünglichen Richtlinie zurückkehren können.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf "Manage Access Policies".
3. Klicken Sie auf den Namen der Zugriffsrichtlinie, die geändert werden soll.
4. Klicken Sie in der Richtlinientabelle auf die Verknüpfung "Richtlinie".
5. Klicken Sie auf "Speichern unter", und geben Sie einen anwenderdefinierten Richtliniennamen ein.
6. Klicken Sie auf "Speichern".
7. Wenn die anwenderdefinierte Richtlinie eine vordefinierte Richtlinie ersetzen soll, öffnen Sie die vordefinierte Richtlinie, und klicken Sie auf "Deaktivieren". Klicken Sie dann auf "Speichern".

Hinweis: Ihre anwenderdefinierte Richtlinie kann nun angepasst werden.

Gewähren oder widerrufen einer Aktion für eine Standardgruppe

Sie können einer Standardgruppe eine neue Aktion gewähren. Sie können auch eine vordefinierte Aktion von einer Standardgruppe widerrufen.

Gehen Sie folgendermaßen vor:

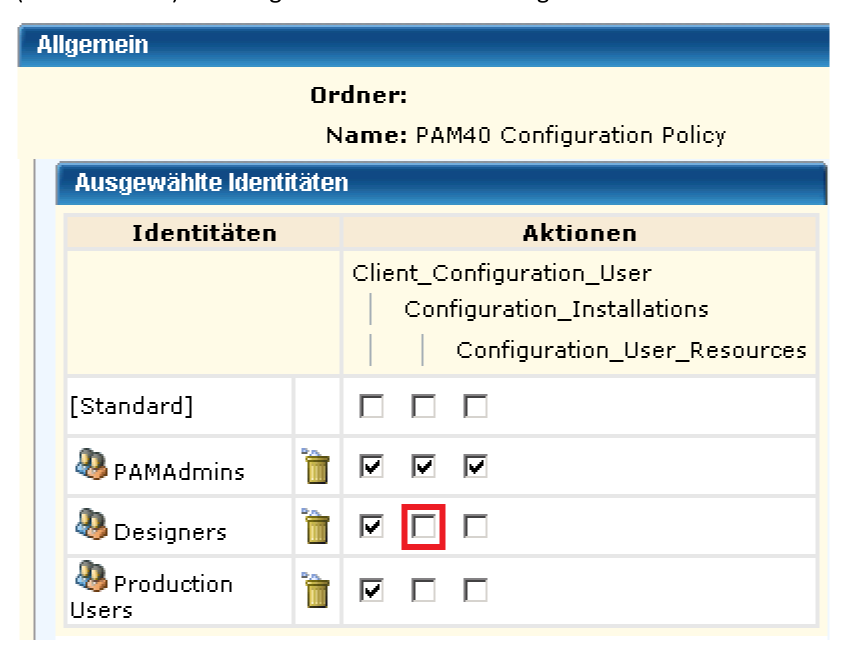
1. Öffnen Sie die anwenderdefinierte Richtlinie, die Sie dafür erstellt haben.
2. Klicken Sie in der Designerzeile für "Ausgewählte Identitäten" auf die Aktion, die Sie identifiziert haben oder löschen Sie sie.

   Hinweis: Weitere Beispiel finden Sie unter Beispiel: Designern die Ausführung von Installationen gewähren (siehe Seite 90).
3. Klicken Sie auf "Speichern".

   Ihre anwenderdefinierte Richtlinie ist wirksam, wenn CA EEM das nächste Mal Aktualisierungen an CA Process Automation sendet.

Beispiel: Designern die Ausführung von Installationen gewähren

Standardmäßig haben Designer keinen Zugriff auf das Auswahlmenü "Installation" auf der Registerkarte "Konfiguration". Sie können den Anwendern in der Gruppe "Designer" die Installation von Agenten gewähren. Überprüfen Sie "Configuration_Installations" (Installationen) für Designer in der PAM40-Konfigurationsrichtlinie.



Beispiel: Designern die Fähigkeit zum Konfigurieren von Gruppen für anwenderspezifische Operatoren gewähren

Standardmäßig dürfen Designer folgende Aktionen auf Gruppen für anwenderspezifische Operatoren nicht ausführen:

- Sperren der Gruppenkonfiguration für einen anwenderspezifischen Operator
- Definieren einer Gruppe mit entsprechenden Variablen für einen Satz von anwenderspezifischen Operatoren
- Entsperren der Gruppenkonfiguration, Veröffentlichen der Gruppe

Veröffentlichte anwenderspezifische Operatorgruppen werden auf der Registerkarte "Modul" im Konfigurationsbrowser angezeigt.

Sie können Inhaltsdesignern die Berechtigung gewähren, anwenderspezifische Operatorgruppen zu erstellen und zu veröffentlichen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei CA EEM an.
2. Klicken Sie auf "Manage Access Policies".

3. Öffnen Sie die Gruppenkonfigurationsrichtlinie.

   a. Klicken Sie auf "Gruppenkonfiguration".

   b. Klicken Sie auf die Verknüpfung der PAM40-Gruppenkonfigurationsrichtlinie.

4. Fügen Sie die Anwendungsgruppe "Designer" zur Liste "Ausgewählte Identitäten" hinzu.

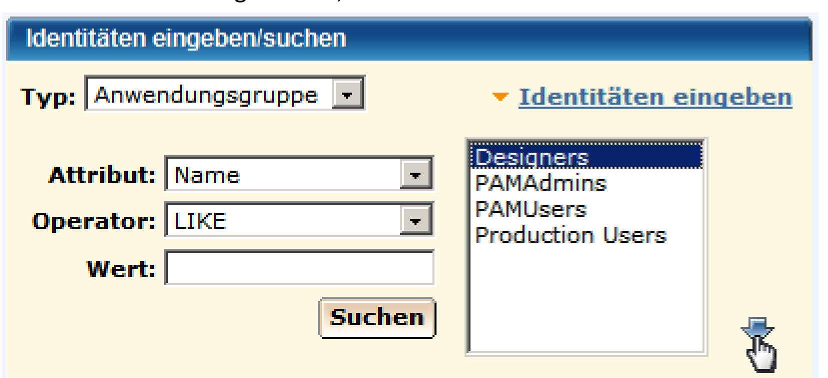
   a. Wählen Sie in der Drop-down-Liste "Typ" die Option "Anwendungsgruppe".

   b. Klicken Sie auf "Identitäten suchen".

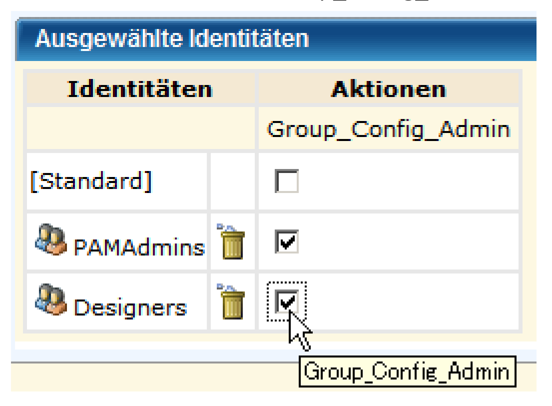
   c. Akzeptieren Sie die Standardeingaben für die folgenden Felder, klicken Sie dann auf "Suchen":

      - **Attribut:** Name
      - **Operator:** WIE
      - **Wert:** Dieses Feld ist standardmäßig leer.

   d. Wählen Sie "Designer" aus, und klicken Sie auf den Nach-unten-Pfeil:



5. Wählen Sie die Aktion "Group_Config_Admin" für die Gruppe "Designer" aus.



6. Klicken Sie auf "Speichern".

So beschränken Sie den Zugriff nach Umgebungen

Die Standardgruppen "Designer" und "Produktionsanwender" wurden für den typischen Fall entworfen, in dem es zwei Umgebungen gibt:

- Designumgebung (Standardumgebung)
- Produktionsumgebung (anwenderspezifische Umgebung)

Mitglieder der Gruppe "Designer" erstellen die automatischen Business-Prozesse in der Designumgebung. Designer entwerfen zum Beispiel Prozesse, Interaktionsauftragsformulare und Datensätze.

Mitglieder der Gruppe "Produktionsanwender" verwenden die entworfenen Prozesse, Formulare und Datensätze. Zum Beispiel starten Produktionsanwender Prozesse, prüfen Datensätze und antworten auf Interaktionsaufträge.

Sie können folgende Richtlinien als anwenderdefinierte Richtlinien speichern, um die Gruppe "Designer" auf die Designumgebung und die Gruppe "Produktionsanwender" auf die Produktionsumgebung zu beschränken.

- Agenda
- Datensatz
- Prozess
- Ressourcen
- Startauftragsformular

Beispiel: Umgebungsfilter

Sie können den Zugriff auf Ablaufpläne nach Umgebungen beschränken. Zum Beispiel können Sie die Standardumgebung für Design verwenden und eine Produktionsumgebung hinzufügen, um die Prozesse und die zugehörigen Objekte, die zur Produktion übertragen wurden, zu verwenden.

Der folgende Beispielfilter für Ablaufpläne beschränkt Mitglieder der Gruppe "Designer" auf die Standardumgebung. Mitglieder der Gruppe "Produktionsanwender" werden auf die Produktionsumgebung beschränkt.

Name/Beschreibung	RessourceKlassenName	Filter
Custom Schedule Policy with Environment Restrictions Restrict Schedule automation object for Designer group to Default Environment and Production User group to Production Environment	Agenda	**WHERE** ((ug:Name == val:Designers **AND** req:action {} val:Control **AND** name:Environment == val:Default Environment) **OR** (ug:Name == val:Production Users **AND** req:action {} val:Control **AND** name:Environment == val:Production Environment))

Sie können Richtlinien anpassen, die auf folgenden Standardrichtlinien mit ähnlichen Filtern basieren:

- PAM40-Datensatzrichtlinie
- PAM40-Prozessrichtlinie
- PAM40-Startauftragsformularrichtlinie
- PAM40-Ressourcenrichtlinie

Öffnen Sie die Standardrichtlinie. Speichern Sie sie als anwenderdefinierte Richtlinie ab. Ändern Sie den Typ auf "Zugriffsrichtlinie". Fügen Sie dann den Filter hinzu.

So passen Sie den Zugriff mit einer anwenderspezifischen Gruppe an

Der grundlegende Vorgang für das Anpassen des Zugriffs mit einer anwenderspezifischen Gruppe:

1. Erstellen einer anwenderspezifischen Gruppe (siehe Seite 93).
2. Hinzufügen einer anwenderspezifischen Gruppe zu einer Standardrichtlinie (siehe Seite 95).

   Hier gewähren Sie der anwenderspezifischen Gruppe Berechtigungen für angegebene Aktionen.
3. Zuweisen einer anwenderspezifischen Gruppe an Anwenderkonten (siehe Seite 96).

   Sie können einem Anwenderkonto mehr als eine Gruppe zuweisen, um Berechtigungen für diesen Anwender zu erweitern.

Hinweis: Beispiele für diesen Vorgang finden Sie unter So führen Sie eine Transition von in Active Directory verwendete Rollen zu CA EEM durch (siehe Seite 119).

Erstellen einer anwenderspezifischen Gruppe

Sie können eine anwenderspezifische Anwendungsgruppe in CA EEM erstellen. Um dieser Gruppe Rechte zu gewähren, fügen Sie die Gruppe zu Richtlinien hinzu, und wählen Sie die entsprechende Aktion aus. Weisen Sie die Gruppe danach einzelnen Anwenderkonten zu.

Hinweis: Ob Sie einer Richtlinie eine anwenderspezifische Gruppe hinzufügen müssen ist davon abhängig, ob die Gruppe auf einer vorhandenen Gruppe basiert.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte Identitäten verwalten.
3. Klicken Sie auf Gruppen.

4. Klicken Sie im Bereich Gruppen neben Anwendungsgruppen auf die Schaltfläche "Neue Anwendungsgruppe", um eine anwenderspezifische Gruppe zu erstellen.
5. Geben Sie im Feld Name einen Namen für die Gruppe ein.
6. (Optional) Geben Sie eine Beschreibung für die Gruppe ein.
7. (Optional) Wählen Sie in der Auswahlgruppe Anwendungsgruppenmitgliedschaft "PAMUsers" aus, um Berechtigungen für Basiszugriff einzuschließen. In diesem Fall können Sie die Berechtigungen, die Sie erteilen, auf diese anwenderspezifische Gruppe beschränken. Berechtigungen, die der Gruppe "PAMUsers" zugewiesen sind, müssen Sie nicht extra gewähren.

   Hinweis: Wenn Sie den Bereich Ausgewählte Benutzergruppen leer lassen, muss die anwenderspezifische Gruppe Berechtigungen für Basiszugriff haben.
8. Klicken Sie auf "Speichern".

   Das Produkt zeigt die neue Gruppe für die Auswahl als Anwendungsgruppe an, wenn Sie neue Anwender definieren.
9. (Optional) Wählen Sie unter Gruppen suchen Anwendungsgruppen anzeigen aus, und klicken Sie auf Los.

   Das Produkt zeigt Ihre neue Gruppe mit anderen Gruppen (einschließlich der Standardgruppen) an.
10. Klicken Sie auf Schließen.

Weitere Informationen:

Hinzufügen einer anwenderspezifischen Gruppe zu einer Standardrichtlinie (siehe Seite 95)

Hinzufügen einer anwenderspezifischen Gruppe zu einer Standardrichtlinie

Eine einfache Methode, um Zugriffsberechtigungen anzupassen, besteht darin, anwenderspezifische Gruppen zu erstellen und jene Gruppen den ausgewählten Standardrichtlinien hinzuzufügen. Mit dieser Vorgehensweise erstellen Sie keine anwenderspezifischen Richtlinien. Sie identifizieren die Aktionen, oder Berechtigungen, in den Standardrichtlinien, die Mitglieder benötigen, die Sie der anwenderspezifischen Gruppe zuweisen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Erstellen Sie eine anwenderspezifische Gruppe für Anwender, die die gleichen Aufgaben in CA Process Automation durchführen sollen.
   a. Klicken Sie auf die Registerkarte "Identitäten verwalten".
   b. Klicken Sie auf "Gruppen".
   c. Klicken Sie auf "Neue Anwendungsgruppe".
   d. Geben Sie den Namen der Gruppe ein.
   e. Fügen Sie keine Anwendungsgruppenmitgliedschaft hinzu.
   f. Klicken Sie auf "Speichern".
3. Öffnen Sie die Standardrichtlinie, die die Aktion enthält, die Sie gewähren möchten.
   a. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".
   b. Klicken Sie unter "Access Policies" auf die gewünschte Ressourcenklasse.
   c. Klicken Sie in der Richtlinientabelle auf den Link für die Richtlinie, die Sie aktualisieren möchten.

      Die ausgewählte Richtlinie wird geöffnet.
4. Gewähren Sie der anwenderspezifischen Gruppe eine ausgewählte Berechtigung.
   a. Wählen Sie unter "Enter/Search Identities" in der Dropdown-Liste "Typ" die Option "Application Group" aus, und klicken Sie auf "Suchen".
   b. Wählen Sie aus der Liste die anwenderspezifische Gruppe aus, und klicken Sie auf den Nach-unten-Pfeil.
   c. Die anwenderspezifische Gruppe wird in der Liste "Selected Identities" angezeigt.
   d. Aktivieren Sie jeweils das Kontrollkästchen neben der zu gewährenden Aktion.
   e. Klicken Sie auf "Speichern".

   Die anwenderspezifische Gruppe wird der ausgewählten Richtlinie hinzugefügt.

Zuweisen einer anwenderspezifischen Gruppe an Anwenderkonten

Sie können eine anwenderspezifische Gruppe (Rolle) zu einem Anwenderkonto zuweisen, während dieses Anwenderkonto erstellt wird. Oder Sie können ein vorhandenes Anwenderkonto bearbeiten, um die neue Anwendungsbenutzergruppe hinzuzufügen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Erstellen Sie das Zielanwenderkonto oder greifen Sie darauf zu.
   - Klicken Sie auf "Neuer Benutzer", um ein Anwenderkonto hinzuzufügen.
   - Verwenden Sie "Benutzer suchen", um ein vorhandenes Anwenderkonto abzurufen.
4. Wenn Sie ein neues Konto erstellen, geben Sie die Anwenderkonto-ID in das Namensfeld ein, geben Sie unter "Globaler Benutzer - Details" Informationen über den Anwender an, geben Sie ein temporäres Kennwort ein, und wählen Sie "Kennwort bei nächster Anmeldung ändern" aus.
5. Klicken Sie auf "Anwendungsanwenderdetails hinzufügen".
6. Wählen Sie in "Verfügbare Benutzergruppen" eine anwenderspezifische Gruppe aus, und klicken Sie auf das Symbol ">", um sie in "Ausgewählte Benutzergruppen" zu verschieben.
7. Klicken Sie auf "Speichern" und anschließend auf "Schließen".
8. Wiederholen Sie diese Schritte für jeden Anwender, dem die Berechtigungen der anwenderspezifischen Gruppe erteilt werden soll.
9. Klicken Sie auf "Abmelden".

So passen Sie den Zugriff für einen angegebenen Anwender an

Sie können einschränken, welche Objekte ein angegebener CA Process Automation-Anwender anzeigen kann, und Sie können die Aktionen einschränken, die dieser Anwender ausführen kann. Sie können CA EEM-Regeln erstellen, sodass ein Anwender nur eine Automatisierungsobjektinstanz oder ein Automatisierungsobjekt sehen oder verwenden kann. Dieser Zugriffstyp ist nur möglich, wenn Inhaltsdesigner mit Bibliotheksobjekten in Arbeitsordnern arbeiten. In diesem Fall werden die Release-Versionen von Objekten in einen Release-spezifischen Ordner kopiert, um als vordefinierter Inhalt exportiert zu werden.

Gehen Sie folgendermaßen vor:

1. Richten Sie designerspezifische Ordner ein (siehe Seite 98).
2. Erstellen Sie ein Anwenderkonto ohne Gruppenzuweisung (siehe Seite 98).
3. Fügen Sie die ausgewählten Standardrichtlinien zu den Anwendern hinzu (siehe Seite 100).
4. Erstellen Sie eine anwenderdefinierte Objektrichtlinie mit Pfadberechtigungen (siehe Seite 102).
5. Erstellen Sie eine anwenderdefinierte Richtlinie für einen angegebenen Objekttyp (siehe Seite 103).

Hinweis: Melden Sie sich mit dem angegebenen Anwender bei CA Process Automation an, und überprüfen Sie, ob Sie der Zugriff korrekt ist.

Einrichten von designerspezifischen Ordnern

Sie können die Ordnerstruktur nach Belieben entwerfen. Entwerfen Sie für einen präzise abgestimmten Zugriff die Struktur, sodass Sie einen Pfad zu den Objekten eines spezifischen Typs in der Richtlinie für dieses Automatisierungsobjekt angeben können. Um einen Anwender (oder eine Gruppe) auf bestimmte Objekttypen oder auf bestimmte Objekttypen in angegebenen Projekten zu beschränken, richten Sie eine Ordnerstruktur ein, für die eine solche Einschränkung zulässig ist. Richten Sie zum Beispiel den Ordner "In Bearbeitung" ("Word In Progress" - WIP) mit einem Ordner für jeden Designer ein.

WIP/designer1

Jeder Designer hat einen separaten Arbeitsordner. Jeder Designerordner enthält eine Reihe von Ordnern, einen Ordner für jeden Automatisierungsobjekttyp, an dem der Entwickler arbeitet. Ein Datensatzordner kann Datensätze für mehrere Projekte enthalten, die von einem einzelnen Designer entwickelt wurden.

/project1/releaseVersion1

Jedes Projekt hat einen spezifischen Ordner mit einem Unterordner für jede Release-Version. Wenn eine Release-Version eines Prozesses für die Übertragung zur Produktion bereit ist, kopieren Sie die Objekte aus den Arbeitsordnern in den Ordner der Release-Version. Der Ordner der Release-Version ist der Ordner, den das Produkt als Inhaltspaket exportiert.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA Process Automation, und melden Sie sich an (siehe Seite 18).
2. Klicken Sie auf die Registerkarte "Bibliothek".
3. Wählen Sie den Stammordner aus, klicken Sie auf "Neu", und wählen Sie dann "Ordner" aus.
4. Geben Sie einen Kurznamen für den neuen Ordner ein.
5. Wiederholen Sie diese Schritte entsprechend, um die erforderliche Ordnerstruktur zu erstellen.

Erstellen eines Anwenderkontos ohne Gruppenzuweisung

Sie können ein Anwenderkonto ohne Gruppenzuweisung erstellen. Dies ist Teil des Prozesses zum Erstellen eines präziser abgestimmten Zugriffs, bei dem Sie Anwender auf das Design und das Testen von Objekten eines bestimmten Typs einschränken.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".

3. Klicken Sie auf das Symbol neben "Anwender" im Auswahlmenü "Anwender".

   Die Seite "Neuer Anwender" wird angezeigt.

4. Geben Sie die Anwender-ID an, die dem Anwenderkonto im Namensfeld zugewiesen werden soll.

   Dieser Name ist der Name, den der Anwender bei der Anmeldung in das Feld "Anwendername" eingibt.

5. Geben Sie die globalen Anwenderdetails ein.

   a. Geben Sie den Namen in die Felder "Vorname" und "Nachname" ein.

      Die Titelleiste zeigt diese Werte an, wenn der Anwender sich bei CA Process Automation anmeldet.

   b. Schließen Sie die anderen Felder im Bereich "Allgemein" entsprechend ab.

6. (Optional) Füllen Sie das Feld "Globale Gruppenmitgliedschaft" aus, wenn Sie CA Process Automation mit einem anderen CA Technologies-Produkt, das dieses CA EEM nutzt, verwenden.

7. Geben Sie ein Kennwort ein, das dem Konto im Bereich "Authentifizierung" zugeordnet werden soll, und bestätigen Sie das Kennwort.

   Geben Sie den Anwendern das temporäre Kennwort, das Sie konfiguriert haben, sodass sie ihre eigenen Kennwörter ändern können.

8. (Optional) Füllen Sie die verbleibenden Felder auf der Seite "Neuer Anwender" aus.

9. Klicken Sie auf "Speichern" und anschließend auf "Schließen".

10. Klicken Sie auf "Abmelden".

Hinzufügen von Anwendern zu ausgewählten Standardrichtlinien

Sie können CA Process Automation-Berechtigungen einer Anwenderidentität gewähren, indem Sie eine oder beide Aktionen durchführen:

- Weisen Sie dem Anwenderkonto eine Anwendergruppe zu.
- Fügen Sie das Anwenderkonto zu den ausgewählten Richtlinien hinzu. Weisen Sie in jeder Richtlinie ausgewählte Aktionen zur Anwenderidentität zu

Wenn Sie mit einer anwenderspezifischen Richtlinie und mit präzise abgestimmten Anwenderrollen arbeiten, empfehlen wir, dass Sie einen grundlegenden Zugriff gewähren, indem Sie die PAMUsers-Gruppe dem Anwenderkonto zuweisen und diesen Zugriff dann mit Zuordnungen der Richtlinienaktion erweitern.

Wenn Sie es vorziehen, den Zugriff nur mit Richtlinien zu gewähren, beginnen Sie mit dem Angeben des grundlegenden Zugriffs. Fügen Sie den Anwenderkontonamen den folgenden Richtlinien und Aktionen hinzu:

- PAM40-Anwenderanmeldungsrichtlinie: Console_Login (Anwender)
- PAM40-Umgebungsrichtlinie: Environment_Library_User (Anwender)
- PAM40-Bibliotheksbrowserrichtlinie: LibraryBrowser_User (Anwender des Bibliotheksbrowsers)

Sie können einen präzise abgestimmten Zugriff auf die Registerkarte "Vorgänge" gewähren. Sie können den Anwenderzugriff auf angegebene Aktionen auf spezifische Objekttypen beschränken.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte Zugriffsrichtlinien verwalten.
3. Fügen Sie den Anwender der PAM40-Anwenderanmeldungsrichtlinie hinzu.
    a. Klicken Sie unter Zugriffsrichtlinien auf den Link für den Produktanwender.
    b. Klicken Sie in der Richtlinientabelle auf den Link PAM40-Anwenderanmeldungsrichtlinie.
    c. Legen Sie "Typ" auf "**Anwender**" fest, und klicken Sie auf "Identitäten suchen".
    d. Klicken Sie auf Suchen.
    e. Wählen Sie die Anwender-ID aus der angezeigten Liste aus, und klicken Sie auf den Nach-unten-Pfeil.
    f. Wählen Sie Console_Login (Anwender) für den Anwender, den Sie hinzugefügt haben, aus.
    g. Klicken Sie auf "Speichern", und klicken Sie auf "Schließen".

4. Fügen Sie den Anwender der PAM40-Umgebungsrichtlinie hinzu.
    a. Klicken Sie unter Zugriffsrichtlinien auf den Link für die Umgebung.
    b. Klicken Sie in der Richtlinientabelle auf den Link PAM40 Environment Policy.
    c. Legen Sie "Typ" auf "**Anwender**" fest, und klicken Sie auf "Identitäten suchen".
    d. Klicken Sie auf Suchen.
    e. Wählen Sie die Anwender-ID aus der angezeigten Liste aus, und klicken Sie auf den Nach-unten-Pfeil.
    f. Wählen Sie Environment_Library_User (Anwender) für den Anwender, den Sie hinzugefügt haben, aus.
    g. Klicken Sie auf "Speichern", und klicken Sie auf "Schließen".
5. Fügen Sie den Anwender der PAM40-Bibliotheksbrowserrichtlinie hinzu.
    a. Klicken Sie unter Zugriffsrichtlinien auf den Link für den Bibliotheksbrowser.
    b. Klicken Sie in der Richtlinientabelle auf den Link PAM40 Library Browser Policy.
    c. Legen Sie "Typ" auf "**Anwender**" fest, und klicken Sie auf "Identitäten suchen".
    d. Klicken Sie auf Suchen.
    e. Wählen Sie die Anwender-ID aus der angezeigten Liste aus, und klicken Sie auf den Nach-unten-Pfeil.
    f. Wählen Sie LibraryBrowser_User (Anwender des Bibliotheksbrowsers) für den Anwender, den Sie hinzugefügt haben, aus.
    g. Klicken Sie auf "Speichern", und klicken Sie auf "Schließen".
6. Gewähren Sie den Anwenderzugriff auf zwei Objekten auf der Registerkarte "Vorgänge". Fügen Sie den Anwender der PAM40-Vorgangsrichtlinie hinzu, und geben Sie nur zwei Aktionen an.
    a. Klicken Sie unter Zugriffsrichtlinien auf den Link für Vorgänge.
    b. Klicken Sie in der Richtlinientabelle auf den Link PAM40 Operations Policy.
    c. Legen Sie "Typ" auf "**Anwender**" fest, und klicken Sie auf "Identitäten suchen".
    d. Klicken Sie auf Suchen.
    e. Wählen Sie die Anwender-ID aus der angezeigten Liste aus, und klicken Sie auf den Nach-unten-Pfeil.
    f. Wählen Sie Operations_Datasets (Datensätze) für den Anwender, den Sie hinzugefügt haben, aus.
    g. Wählen Sie Operations_Resources (Ressourcen) für den Anwender, den Sie hinzugefügt haben, aus.
    h. Klicken Sie auf "Speichern", und klicken Sie auf "Schließen".

Erstellen einer anwenderdefinierten Objektrichtlinie mit Pfadberechtigungen

Erstellen Sie eine anwenderspezifische Objektzugriffsrichtlinie mit der Zugriffsrichtlinie "Objekt". Die Anzahl von Einträgen, die Sie vornehmen, hängt von der Tiefe des Pfades ab. Geben Sie eine Zeile für jede Pfadebene ein, und beginnen Sie dabei mit dem Stammordner (/).

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".
3. Erstellen Sie eine anwenderspezifische Objektrichtlinie, um einen angegebenen Anwender auf einen angegebenen Pfad in der Bibliothek zu beschränken.
   a. Klicken Sie unter "Zugriffsrichtlinie" auf die Verknüpfung "Neue Zugriffsrichtlinie" für "Objekt".
   b. Geben Sie einen Namen ein.
   c. Wählen Sie als Typ "Zugriffssteuerungsliste" aus, und klicken Sie in der Bestätigungsmeldung auf "OK".
   d. Klicken Sie auf "Identitäten suchen", mit "Benutzer" als "Typ" festgelegt.
   e. Klicken Sie auf "Suche". Wählen Sie die Anwender-ID aus der angezeigten Liste aus, und klicken Sie auf den Nach-rechts-Pfeil.
   f. Geben Sie einen Schrägstrich (/) in das Feld "Ressource hinzufügen" ein, und klicken Sie auf "Hinzufügen".
   g. Geben Sie im gleichen Feld einen Schrägstrich (/) ein, gefolgt von dem Namen des Ordners, der die Objekte enthält, auf die der Anwender eingeschränkt ist. Klicken Sie auf "Hinzufügen".
   h. Wählen Sie "Object_List" (Liste) für den Stammordner (/) aus.
   i. Wählen Sie "Object_List" (Liste) für den /*Ordnerpfad* aus. Wiederholen Sie diesen Schritt, wenn es /*Ordner*/*Unterordnerpfad* gibt.

      Hinweis: Sie können /Ordner/Unterordner* eingeben und "Ressourcennamen als regulären Ausdruck behandeln" auswählen, um alle Ordner einzuschließen, die dem angegebenen Unterordner untergeordnet sind.
   j. Klicken Sie auf "Speichern". Klicken Sie auf "Schließen".

Erstellen einer anwenderdefinierten Richtlinie für einen angegebenen Objekttyp

Erstellen Sie eine Richtlinie für den Objekttyp, auf den sich die Einschränkung bezieht. Geben Sie dann die Aktionen an, die auf dem ausgewählten Objekttyp erlaubt werden sollen. Wählen Sie aus folgenden Richtlinientypen aus:

- Agenda
- Datensatz
- Prozess
- Ressourcen
- Startauftragsformular

Hinweis: Details zu Berechtigungen finden Sie unter Berechtigungsreferenz. (siehe Seite 104)

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".
3. Erstellen Sie eine anwenderdefinierte Richtlinie für den Objekttyp, den Sie einschränken möchten.
   a. Klicken Sie auf die Verknüpfung "Neue Zugriffsrichtlinie" für einen der folgenden Ressourcentypen: Agenda, Datensatz, Prozess, Ressourcen, Startauftragsformular.
   b. Geben Sie einen Namen ein.
   c. Wählen Sie als Typ "Zugriffssteuerungsliste" aus, und klicken Sie in der Bestätigungsmeldung auf "OK".
   d. Klicken Sie auf "Identitäten suchen", mit "Benutzer" als "Typ" festgelegt.
   e. Klicken Sie auf "Suche". Wählen Sie die Anwender-ID aus der angezeigten Liste aus, und klicken Sie auf den Nach-rechts-Pfeil.
   f. Geben Sie im Feld "Ressource hinzufügen" den vollständigen Pfad ein, der den von Ihnen ausgewählten Objekttyp enthält. Klicken Sie auf "Hinzufügen".
   g. Geben Sie im gleichen Feld einen Schrägstrich (/) ein, und geben Sie dann den Namen des Ordners ein, der die Objekte enthält, auf die der Anwender beschränkt ist. Klicken Sie auf "Hinzufügen".
   h. Wählen Sie die zu gewährende Berechtigung aus.
      - Agenda: Agenda_Control (Steuerung). "Agenda" bezieht sich auf Ablaufpläne.
      - Datensatz: Dataset_Inspect (Untersuchen), Dataset_Modify (Ändern).
      - Prozess: Process_Control (Steuerung), Process_Monitor (Überwachen), Process_Start (Start).

- Ressourcen: Resources_Control

i. Klicken Sie auf "Speichern". Klicken Sie auf "Schließen".

4. (Optional) Fügen Sie einen Filter hinzu, um nach Umgebungen zu beschränken.
5. Wiederholen Sie diesen Vorgang für abhängige Objekte. Beispiel: Datensätze. Datensätze sind nur im Zusammenhang eines anderen Objekttyps aussagekräftig. Wenn Sie "Datensätze" ausgewählt haben, erstellen Sie eine andere Richtlinie, z. B. für "Ressourcen".

Berechtigungsreferenz

In den folgenden Tabellen sind alle Berechtigungen mit Abhängigkeiten und Filtern aufgeführt:

- Berechtigungen nach Registerkarten (siehe Seite 104)
- Berechtigungen für Automatisierungsobjekte (siehe Seite 111)
- Abhängigkeiten der Berechtigungen (siehe Seite 114)
- Filter für Berechtigungen (siehe Seite 117)

Berechtigungen nach Registerkarten

Die Aktionen, die für vordefinierte CA EEM-Richtlinien ausgewählt sind, gewähren Berechtigungen für Registerkarten, Auswahlmenüs, Ordner und Automatisierungsobjekte. Die folgenden Tabellen beschreiben die Berechtigungen, die die einzelnen Aktionen den Gruppen (Identitäten) in den entsprechenden Ressourcenrichtlinien gewähren.

Wenn Sie anwenderspezifische Richtlinien auf der Grundlage dieser Ressourcenklassen erstellen, orientieren Sie sich beim Zuweisen von Berechtigungen an den entsprechenden Tabellen.

Registerkarte "Startseite"

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
Console_Login (Anwender)	Product User	Anmelden bei CA Process Automation und Verwenden der Registerkarte "Startseite".

Registerkarte "Bibliothek"

In der folgenden Tabelle sind die Berechtigungen von der niedrigsten bis zur höchsten Ebene angeordnet angezeigt. Um die Registerkarte "Bibliothek" anzuzeigen, müssen Sie über die Berechtigung "LibraryBrowser_User" sowie entweder die Berechtigung "Environment_Library_User" oder die Berechtigung "Environment_Library_Admin" verfügen. Weitere Informationen finden Sie unter Abhängigkeiten der Berechtigungen (siehe Seite 114).

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für Richtlinie**	**Berechtigungen**
LibraryBrowser_User (Anwender des Bibliotheksbrowsers)	LibraryBrowser (Bibliotheksbrowser)	Anzeigen des Zugriffs auf die Registerkarte "Bibliothek".
Object_List (Liste)	Objekt	■ Anzeigen eines Ordners oder Automatisierungsobjekts im Bibliotheksbrowser. ■ Definieren von benutzerdefinierten Bibliotheksansichten.
Environment_Library_User (Anwender)	Umgebung	Voraussetzung für viele Berechtigungen für die Registerkarte "Vorgänge". ■ Zugriff auf Koordinationsrechner, die den Umgebungen hinzugefügt wurden. ■ Anzeigen, Exportieren und Suchen von Automatisierungsobjekten in der Registerkarte "Bibliothek", wenn der Zugriff festgelegt ist.
Object_Read (Lesen)	Objekt	Navigieren durch einen Ordnerpfad und Öffnen eines Automatisierungsobjekts im entsprechenden Designer oder Viewer. *Implizit:* Liste
Object_Edit (Bearbeiten)	Objekt	Bearbeiten eines Ordners oder eines Automatisierungsobjekts in einem Ordner. *Implizit:* Lesen, Liste
Object_Delete (Löschen)	Objekt	Löschen eines Ordners oder Löschen eines einem Ordner hinzugefügten Automatisierungsobjekts. *Implizit:* Bearbeiten, Lesen, Liste
Object_Admin (Admin)	Objekt	Erstellen eines Ordners oder eines Automatisierungsobjekts. *Implizit:* Löschen, Bearbeiten, Lesen, Liste

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
Environment_Library_Admin (Inhaltsadministrator)	Umgebung	Erstellen, Löschen, Bearbeiten, Lesen und Auflisten aller Automatisierungsobjekte in der Registerkarte "Bibliothek".
Group_Config_Admin	Gruppenkonfiguration	Zugriff auf die Registerkarte "Gruppenkonfiguration". Unter Berechtigungen für Automatisierungsobjekte (siehe Seite 111) finden Sie Informationen zu gewährten Berechtigungen für anwenderspezifische Operatoren.

Registerkarte "Designer"

Anwendern mit Zugriff auf die Registerkarte "Designer" wird normalerweise auch Zugriff auf die Registerkarte "Bibliothek" gewährt. Designer benötigen mindestens folgende Berechtigungen für die Registerkarte "Bibliothek", um einen entworfenen Prozess zu speichern:

- LibraryBrowser_User
- Environment_Library_User
- Object_Edit (beinhaltet die Berechtigungen "Object_List" und "Object_Read")

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
Designer_User (Designer-Anwender)	Designer	Anzeigen des Zugriffs auf die Registerkarte "Designer".

Registerkarte "Vorgänge" und Auswahlmenüs

Designer müssen Zugriff auf die Registerkarte "Vorgänge" in der Designumgebung haben, und Produktionsanwender müssen Zugriff auf die Registerkarte "Vorgänge" in der Produktionsumgebung haben. Um die Registerkarte "Vorgänge" anzuzeigen, müssen Sie über die Berechtigung "Environment_Library_User" oder "Environment_Library_Admin" verfügen. Weitere Informationen finden Sie unter Abhängigkeiten der Berechtigungen (siehe Seite 114).

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für Richtlinie**	**Berechtigungen**
Operations_Process_Watch (Prozessüberwachung)	Vorgänge	■ Öffnen des Auswahlmenüs "Prozessüberwachung" in der Registerkarte "Vorgänge". ■ Anzeigen aller Prozesse im ausgewählten Zustand, aktiver Ablaufpläne, aktiver Operatoren und Anwenderanfragen.
Process_Monitor (Überwachen)	Prozess	■ Öffnen eines Prozesses im Prozess-Designer. ■ Überwachen des Fortschritts. ■ Festlegen von Haltepunkten. *Implizit:* Liste
Process_Start (Starten)	Prozess	Starten einer Prozessinstanz. *Implizit:* Monitor, Liste
Process_Control (Steuerelement)	Prozess	Unterbrechen, neu Starten, Wiederaufnehmen oder Abbrechen von Prozessinstanzen. *Implizit:* Start, Monitor, Liste
Operations_Schedules (Ablaufpläne)	Vorgänge	Anzeigen der Verknüpfung "Aktive Ablaufpläne" auf der Registerkarte "Vorgänge".
Agenda_Control (Steuerelement)	Agenda	Aktivieren und Deaktivieren von Ablaufplänen auf einem Kontaktpunkt. *Implizit:* Lesen, Liste
Operations_Datasets (Datensätze)	Vorgänge	Öffnen des Auswahlmenüs "Datensätze" auf der Registerkarte "Vorgänge".
Dataset_Inspect (Untersuchen)	Datensatz	Anzeigen eines Datensatzobjekts und Lesen von Variablenwerten im Datensatz. *Implizit:* Liste

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
Dataset_Modify (Ändern)	Datensatz	Erstellen, Bearbeiten und Löschen des Objekts "Datensatz". *Implizit:* Untersuchen, Lesen, Liste
Operations_Resources (Ressourcen)	Vorgänge	Öffnen des Auswahlmenüs "Ressourcen" auf der Registerkarte "Vorgänge".
Resources_Control (Steuerelement)	Ressourcen	■ Sperren, Entsperren, Übernehmen, Zurückgeben oder Hinzufügen eines Parameters zu einer Ressource. ■ Hinzufügen oder Entfernen einer Ressourceneinheit. *Implizit:* Lesen, Liste
Operations_User_Requests (Anwenderanfragen)	Vorgänge	Öffnen des Auswahlmenüs "Anwenderanfragen" auf der Registerkarte "Vorgänge".
Operations_Content_Packages (vordefinierte Inhalte)	Vorgänge	Öffnen des Auswahlmenüs "Vordefinierte Inhalte" auf der Registerkarte "Vorgänge".
Operations_Task_List (Aufgabenliste)	Vorgänge	■ Verwenden der Verknüpfung "Aufgabenliste" auf der Registerkarte "Vorgänge" und Anzeigen von Aufgaben für sich, für Ihre Gruppe oder für eine andere Gruppe. ■ Zugriff auf Ihre eigenen Aufgaben auf der Registerkarte "Startseite".
StartRequestForm_Dequeue (Aus Warteschlange entfernen)	Startauftragsformular	Entfernen eines Prozesses, der durch ein Startauftragsformular in die Warteschlange gestellt wurde, aus der Warteschlange. *Implizit:* Start, Liste
StartRequestForm_Start (Starten)	Startauftragsformular	Starten einer Aufgabe, die ein Startauftragsformular definiert. *Implizit:* Liste
Ausführen	Kontaktpunktsicherheit	Ausführen von Skripten oder Programmen in Operatoren. Das Produkt leitet die betroffenen Operatoren aus den angegebenen Operatorkategorien ab. Die Auswirkung tritt auf, wenn das Ziel ein angegebener Kontaktpunkt in einer angegebenen Umgebung ist.

Registerkarte "Berichte"

In der folgenden Tabelle sind die Aktionen aufgelistet, die für die Verwendung der Registerkarte "Berichte" relevant sind.

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
Reports_User (Berichtsanwender)	Berichte	■ Öffnen der Registerkarte "Berichte" ■ Hochladen von anwenderspezifischen Berichten ■ Anzeigen oder Löschen von vordefinierten, freigegebenen oder privaten Berichten.

Registerkarte "Konfiguration" und Auswahlmenüs

In der folgenden Tabelle sind die Aktionen aufgelistet, die Auswirkungen auf Berechtigungen für die Registerkarte "Konfiguration" haben. Um den Konfigurationsbrowser auf der Registerkarte "Konfiguration" anzuzeigen, müssen Sie über die Berechtigung "Client_Configuration_User" verfügen. Weitere Informationen finden Sie unter Abhängigkeiten der Berechtigungen (siehe Seite 114).

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
Client_Configuration_User (Konfigurationsbrowser anzeigen)	Konfigurationsbrowse r	Anzeigen der Registerkarte "Konfiguration" im Konfigurationsbrowser.
Environment_Configuration_Admin (Konfigurationsadministrator)	Umgebung	■ "Neue Gruppe hinzufügen", "Kontaktpunkt hinzufügen" und "Hostgruppe hinzufügen" im Konfigurationsbrowser. ■ Bearbeiten der Konfiguration auf Umgebungsebene. Dazu gehören Sicherheit, Eigenschaften, Operatorkategorien, anwenderspezifische Operatorgruppen und Auslöser.

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
Domain_Admin (Administrator)	Domäne	■ Sperren bzw. Entsperren der Domäne, Hinzufügen von "Umgebung" und Aufrufen von "Gebündelte Agentenentfernung" und "Gebündelte Entfernung von Kontaktpunkten" im Auswahlmenü "Konfigurationsbrowser". ■ Bearbeiten der Konfiguration auf Domänenebene. Dazu gehören Sicherheit, Eigenschaften, Operatorkategorien, anwenderspezifische Operatorgruppen und Auslöser. ■ Aktualisieren des Ordners "Koordinationsrechnerressourcen" und der Inhalte des Ordners "Agentenressourcen" im Auswahlmenü "Anwenderressourcen verwalten".
Configuration_User_Resources (Anwenderressourcen)	Konfigurationsbrowse r	Öffnen des Auswahlmenüs "Anwenderressourcen verwalten" auf der Registerkarte "Konfiguration" und Aktualisieren der Inhalte des Ordners "Anwenderressourcen".
Configuration_Installations (Installationen)	Konfigurationsbrowse r	Öffnen des Auswahlmenüs "Installation" auf der Registerkarte "Konfiguration" und Starten der Installation eines Agenten, Koordinationsrechners oder Cluster-Knotens eines Koordinationsrechners.

Weitere Informationen:

Abhängigkeiten der Berechtigungen (siehe Seite 114)

Berechtigungen für Automatisierungsobjekte

Die folgende Tabelle beschreibt Berechtigungen, die Sie für verschiedene Automatisierungsobjekte mithilfe von anwenderspezifischen CA EEM-Richtlinien erteilen können. Sie können für alle Anwendungsgruppen in CA EEM Berechtigungen erteilen. Für Zugriff auf Automatisierungsobjekte und Ordner auf einem Koordinationsrechner in einer Umgebung ist Anwender- oder Inhaltsadministratoren-Zugriff in der Umgebungsrichtlinie erforderlich. "Umgebung" ist die übergeordnete Ressourcenklasse der Ressourcenklassen für Automatisierungsobjekte.

Einige Berechtigungen schließen implizit andere Berechtigungen ein. Wenn Sie eine bestimmte Berechtigung auswählen, werden gleichzeitig implizite Berechtigungen ausgewählt. Wenn Sie eine explizite Berechtigung erteilen, erteilen Sie implizit alle anderen in der Berechtigungshierarchie darunterliegenden Berechtigungen.

Wenn Sie eine implizite Berechtigung aberkennen, erkennen Sie alle anderen in der Berechtigungshierarchie darüber liegenden Berechtigungen ab. Die Berechtigung "Liste" ist implizit in jeder anderen Berechtigung enthalten und von keiner anderen Berechtigung abhängig. Sie können alle Berechtigungen für eine Gruppe in Bezug auf einen Ordner mit einer anwenderspezifischen Objekt-Richtlinie ablehnen, die Berechtigungen mit "Liste" ablehnt. Durch das Widerrufen der Berechtigung "Liste" werden alle anderen Berechtigungen für ein Automatisierungsobjekt widerrufen. Durch das Widerrufen anderer Berechtigungen wird die Berechtigung "Liste" jedoch nie widerrufen.

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für Richtlinie**	**Berechtigungen**
Object_Admin (Admin)	Objekt	Erstellen eines Ordners oder eines Automatisierungsobjekts. **Implizit:** Löschen, Bearbeiten, Lesen, Liste
Object_Delete (Löschen)	Objekt	Löschen eines Ordners oder Löschen eines einem Ordner hinzugefügten Automatisierungsobjekts. **Implizit:** Bearbeiten, Lesen, Liste
Object_Edit (Bearbeiten)	Objekt	Bearbeiten eines Ordners oder eines Automatisierungsobjekts in einem Ordner. **Implizit:** Lesen, Liste
Object_Read (Lesen)	Objekt	Navigieren durch einen Ordnerpfad und Öffnen eines Automatisierungsobjekts im entsprechenden Designer oder Viewer. **Implizit:** Liste

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für Richtlinie**	**Berechtigungen**
Object_List (Liste)	Objekt	Anzeigen eines Ordners oder Automatisierungsobjekts im Bibliotheksbrowser. Definieren anwenderspezifischer Ansichten der Bibliothek.
Environment_Library_Admin (Inhaltsadministrator)	Umgebung	Erstellen, Löschen, Bearbeiten, Lesen und Auflisten aller Automatisierungsobjekte.
Environment_Library_User (Anwender)	Umgebung	Anzeigen, Exportieren, Suchen von Automatisierungsobjekten, wenn der Zugriff festgelegt ist. **Hinweis**: Implizit vererbbar durch Ressourcenklassen für Automatisierungsobjekte
Agenda_Control (Steuerelement)	Agenda	Aktivieren und Deaktivieren von Ablaufplänen auf einem Kontaktpunkt. **Implizit:** Lesen, Liste
Dataset_Modify (Ändern)	Datensatz	Erstellen, Bearbeiten und Löschen des Objekts "Datensatz". **Implizit:** Untersuchen, Lesen, Liste
Dataset_Inspect (Untersuchen)	Datensatz	Anzeigen eines Objekts "Datensatz" und Lesen von Variablenwerten im Datensatz. **Implizit:** Liste
Process_Control (Steuerelement)	Prozess	Unterbrechen, Neustarten, Fortfahren oder Abbrechen von Instanzen eines Prozesses. **Implizit:** Start, Monitor, Liste
Process_Start (Starten)	Prozess	Starten einer Instanz eines Prozesses. **Implizit:** Monitor, Liste
Process_Monitor (Überwachen)	Prozess	Öffnen einer laufenden Instanz eines Prozesses im Prozess-Designer, Überwachen des Fortschritts und Festlegen von Haltepunkten. **Implizit:** Liste
Resources_Control (Steuerelement)	Ressourcen	Sperren, Entsperren, Übernehmen, Zurückgeben oder Hinzufügen eines Parameters zu einer Ressource. Hinzufügen oder Entfernen einer Ressourceneinheit. **Implizit:** Lesen, Liste

Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für Richtlinie	Berechtigungen
StartRequestForm_Dequeue (Aus Warteschlange entfernen)	Startauftragsformular	Entfernen eines Prozesses aus der Warteschlange, der von einem Startauftragsformular in die Warteschlange gestellt wurde. **Implizit:** Start, Liste
StartRequestForm_Start (Starten)	Startauftragsformular	Starten einer Aufgabe, die von einem Startauftragsformular definiert wurde. **Implizit:** Liste
Ausführen	Kontaktpunktsicherheit	Ausführen von Skripten oder Programmen in Operatoren, die von angegebenen Operatorkategorien, die auf die angegebenen Kontaktpunkte in einer angegebenen Umgebung verweisen, abgeleitet sind.
Group_Config_Admin	Gruppenkonfiguration	Definieren von Parametern für eine anwenderspezifische Operatorgruppe, wenn ein anwenderspezifischer Operator definiert wird. **Gehen Sie folgendermaßen vor:** 1. Sperren Sie die anwenderspezifische Operatorgruppe auf der Registerkarte "Gruppenkonfiguration". 2. Fügen Sie Seiten und Variablen hinzu. 3. Speichern der Konfiguration. 4. Entsperren Sie die Gruppe "Anwenderspezifischer Operator". "Entsperren" veröffentlicht die Konfiguration der benannten Gruppe "Anwenderspezifischer Operator". "Veröffentlichung" stellt die Gruppenkonfiguration auf der Registerkarte "Module" im Konfigurationsbrowser auf Domänen- und Umgebungsebene zur Verfügung.

Weitere Informationen:

Abhängigkeiten der Berechtigungen (siehe Seite 114)

Abhängigkeiten der Berechtigungen

Die folgende Tabelle beschreibt die abhängige Ressourcenklassenaktion (Berechtigung) für jede Ressourcenklassenaktion auf den vordefinierten CA EEM-Richtlinien für CA Process Automation.

Berücksichtigen Sie die Abhängigkeiten, wenn Sie Anwenderkonten nur anwenderdefinierte Gruppen (ohne PAMUsers) zuweisen.

Wie in der Tabelle zusammengefasst können Sie einen Aktionsschlüssel in einer anwenderdefinierten Richtlinie für eine Ressourcenklasse zu einer anwenderspezifischen Gruppe zuweisen. Wenn Sie so eine anwenderdefinierte Richtlinie erstellen, weisen Sie diese anwenderspezifische Gruppe einem abhängigen Aktionsschlüssel zu.

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für anwenderdefinierte Richtlinien**	**Abhängiger Aktionsschlüssel (Lokalisierter Name)**
Console_Login (Anwender)	Product User	
Reports_User (Berichtsanwender)	Berichte	Console_Login (Anwender)
Environment_Library_User (Anwender)	Umgebung	Console_Login (Anwender)
Environment_Library_Admin (Inhaltsadministrator)	Umgebung	Console_Login (Anwender)
Environment_Configuration_Admin (Konfigurations-Administrator)	Umgebung	Console_Login (Anwender)
Domain_Admin (Administrator)	Domäne	Console_Login (Anwender)
Client_Configuration_User (Konfigurationsbrowser anzeigen)	Konfigurationsbrowser	Console_Login (Anwender)
Configuration_User_Resources (Anwenderressourcen)	Konfigurationsbrowser	■ Console_Login (Anwender) ■ Client_Configuration_User (Konfigurationsbrowser anzeigen) ■ Domain_Admin (Administrator) für den Zugriff auf die Ordner "Agentenressourcen" und "Koordinationsrechnerressourcen".

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für anwenderdefinierte Richtlinien**	**Abhängiger Aktionsschlüssel (Lokalisierter Name)**
Configuration_Installations (Installationen)	Konfigurationsbrowse r	Console_Login (Anwender)
LibraryBrowser_User (Anwender des Bibliotheksbrowsers)	Bibliotheksbrowser	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)
Operations_User_Requests (Anwenderanfragen)	Vorgänge	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)
Operations_Process_Watch (Prozessüberwachung)	Vorgänge	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)
Operations_Task_List (Aufgabenliste)	Vorgänge	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)
Operations_Schedules (Ablaufpläne)	Vorgänge	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)
Operations_Resources (Ressourcen)	Vorgänge	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)
Operations_Datasets (Datensätze)	Vorgänge	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)
Operations_Content Packages (Vordefinierte Inhalte)	Vorgänge	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) oder Environment_Library_Admin (Inhaltsadministrator)

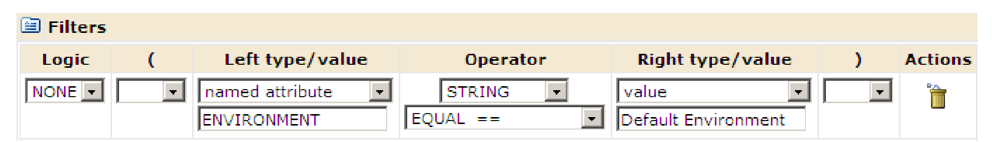
Aktionsschlüssel (Lokalisierter Name)	Ressourcenklasse für anwenderdefinierte Richtlinien	Abhängiger Aktionsschlüssel (Lokalisierter Name)
■ Object_List (Liste) ■ Object_Read (Lesen) ■ Object_Edit (Bearbeiten) ■ Object_Delete (Löschen) ■ Object_Admin (Admin)	Objekt	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender)
Agenda_Control (Kontrolle)	Agenda	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) ■ Object_List (Liste) mit Ressource */folder* **Hinweis:** Wenn das Objekt im Stammordner erstellt wird, muss "Object_List" nicht angegeben werden.
■ Dataset_Inspect (Untersuchen) ■ Dataset_Modify (Ändern)	Datensatz	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) ■ Object_List (Liste) mit Ressource */folder* **Hinweis:** Wenn das Objekt im Stammordner erstellt wird, muss "Object_List" nicht angegeben werden.
■ Process_Control (Kontrolle) ■ Process_Monitor (Monitor) ■ Process_Start (Start)	Prozess	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) ■ Object_List (Liste) mit Ressource */folder* **Hinweis:** Wenn das Objekt im Stammordner erstellt wird, muss "Object_List" nicht angegeben werden.
Resources_Control (Kontrolle)	Ressourcen	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) ■ Object_List (Liste) mit Ressource */folder* **Hinweis:** Wenn das Objekt im Stammordner erstellt wird, muss "Object_List" nicht angegeben werden.

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für anwenderdefinierte Richtlinien**	**Abhängiger Aktionsschlüssel (Lokalisierter Name)**
■ StartRequestForm_Start (Start) ■ StarRequestForm_Dequeue (Aus der Warteschlange entfernen)	Startauftragsformular	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) ■ Object_List (Liste) mit Ressource */folder* **Hinweis:** Wenn das Objekt im Stammordner erstellt wird, muss "Object_List" nicht angegeben werden.
Ausführen	Kontaktpunktsicherheit	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) ■ Object_List (Liste) mit Ressource */folder* **Hinweis:** Wenn das Objekt im Stammordner erstellt wird, muss "Object_List" nicht angegeben werden.
Group_Config_Admin	Gruppenkonfiguration	■ Console_Login (Anwender) ■ Environment_Library_User (Anwender) ■ Object_List (Liste) mit Ressource */folder* ■ Object_Edit (Bearbeiten) mit Ressource */folder*

Filter für Berechtigungen

CA EEM definiert Berechtigungen als Ressourcenklassen-Aktionen. Sie können optional Filter verwenden, um die Aktionen zu beschränken, die Sie einer Gruppe oder einem Anwender gewähren. Zum Beispiel können Sie Berechtigungen einschränken, sodass sie nur auf die zugewiesene Gruppe in der konfigurierten Umgebung angewendet werden.

Das folgende Filterbeispiel veranschaulicht die Verwendung von "UMGEBUNG" als benanntes Attribut für den Filter. Mit Richtlinien, die mit dem Typ "Zugriffsrichtlinien" definiert sind, können Sie Filter hinzufügen.



Die Aktionen in der folgenden Tabelle gehören zu den Richtlinien, die auf der referenzierten Ressourcenklasse basieren.

Aktionsschlüssel (Lokalisierter Name)	**Ressourcenklasse für Richtlinie**	**Benanntes Attribut für Filter**
Object_List (Liste) Object_Read (Lesen) Object_Edit (Bearbeiten) Object_Delete (Löschen) Object_Admin (Admin)	Objekt	SECURITY_CONTEXT_ID SECURITY_CONTEXT_GRP Umgebung OBJECT_TYPE
Agenda_Control (Kontrolle)	Agenda	Umgebung
Dataset_Inspect (Untersuchen) Dataset_Modify (Ändern)	Datensatz	Umgebung
Process_Control (Kontrolle) Process_Monitor (Monitor) Process_Start (Start)	Prozess	SECURITY_CONTEXT_ID SECURITY_CONTEXT_GRP Umgebung
Resources_Control (Kontrolle)	Ressourcen	Umgebung
StartRequestForm_Start (Start) StarRequestForm_Dequeue (Aus der Warteschlange entfernen)	Startauftragsformular	Umgebung
Ausführen	Kontaktpunktsicherheit	Umgebung Kontaktpunkt

So führen Sie eine Transition von in Active Directory verwendete Rollen zu CA EEM durch

Wenn Sie zuvor Microsoft Active Directory (AD) oder LDAP für die Authentifizierung und Autorisierung verwendet haben, können Sie eine Transition zu CA EEM folgendermaßen durchführen:

- Erstellen Sie Anwenderkonten. Weisen Sie jedem Konto eine der Standardgruppen zu.

  Hinweis: Weitere Informationen finden Sie unter Überprüfen von Berechtigungen für Standardgruppen (siehe Seite 48).

- Verweisen Sie auf AD als externen Anwenderspeicher.

  Hinweis: Weitere Informationen finden Sie unter Verwalten der Zugriffe für referenzierte Anwenderkonten (siehe Seite 62). Weitere Informationen finden Sie unter Integrieren von Active Directory mit CA EEM.

- Erstellen Sie anwenderspezifische Gruppen, die Ihre AD-Rollen widerspiegeln. Fügen Sie diese Gruppen CA EEM-Richtlinien hinzu und gewähren Sie die erforderlichen Berechtigungen. Erstellen Sie Anwenderkonten. Weisen Sie jedem Konto eine Ihrer anwenderspezifischen Gruppen zu. Dieser Abschnitt beschreibt diese Vorgehensweise.

Angenommen, Sie haben die Sicherheitseinstellungen der Domäne in Active Directory mit diesen Gruppen definiert: ITPAMAdmins, ITPAMUsers, ConfigAdmin, ContentAdmin und EnvironmentUser.

Sicherheitseinstellungen der Domäne

Domänenadministrator	ITPAMAdmins
CA IT PAM-Anwender	ITPAMUsers
Umgebungskonfigurations-Administrator	ConfigAdmin
Umgebungsinhalts-Administrator	ContentAdmin
Umgebungsanwender	EnvironmentUser

Verwenden Sie den folgenden Prozess, um rollenbasierten Zugriff von Active Directory nach CA EEM zu migrieren.

Gehen Sie folgendermaßen vor:

1. Migrieren Sie rollenbasierten Zugriff für Anwender in der Rolle "Domänenadministrator".

   Weitere Informationen finden Sie unter Erstellen von Anwenderkonten für Administratoren (siehe Seite 56).

2. Migrieren Sie rollenbasierten Zugriff für Anwender in der CA Process Automation-Anwenderrolle.

   Weitere Informationen finden Sie unter Erstellen von Anwenderkonten mit grundlegendem Zugriff (siehe Seite 58).

3. Migrieren Sie folgendermaßen rollenbasierten Zugriff für Anwender in der Rolle "Umgebungskonfigurations-Administrator":

   a. Erstellen der anwenderspezifischen ConfigAdmin-Gruppe (siehe Seite 121).

   b. Gewähren von Berechtigungen für die anwenderspezifische ConfigAdmin-Gruppe (siehe Seite 122).

   c. Erstellen von Anwenderkonten für Umgebungskonfigurations-Administratoren (siehe Seite 123).

4. Migrieren Sie folgendermaßen rollenbasierten Zugriff für Anwender in der Rolle "Umgebungsinhalts-Administrator":

   a. Erstellen der anwenderspezifischen ContentAdmin-Gruppe (siehe Seite 124).

   b. Gewähren von Berechtigungen für die anwenderspezifische ContentAdmin-Gruppe (siehe Seite 125).

   c. Erstellen von Anwenderkonten für Umgebungsinhalts-Administratoren (siehe Seite 126).

5. Migrieren Sie rollenbasierten Zugriff für Anwender in der Rolle "Umgebungsanwender".

   Weitere Informationen finden Sie unter Erstellen von Anwenderkonten für Produktionsanwender (siehe Seite 58).

Erstellen der anwenderspezifischen ConfigAdmin-Gruppe

Sie können eine anwenderspezifische Gruppe mit dem Namen "ConfigAdmin" für Anwender in der Rolle "Umgebungskonfigurations-Administrator" erstellen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie in der Registerkarte "Identitäten verwalten" auf "Gruppen" und klicken Sie auf "Neue Anwendungsgruppe".
3. Geben Sie **ConfigAdmin** als den Namen der Gruppe oder einen Namen Ihrer Wahl ein.
4. (Optional) Geben Sie eine Beschreibung für die Gruppe ein.
5. Klicken Sie auf "Speichern".

   Hinweis: Fügen Sie keine Anwendungsgruppenmitgliedschaft hinzu.
6. Klicken Sie auf "Schließen".

Gewähren von Berechtigungen für die Gruppe "Umgebungskonfigurations-Administrator"

Sie können der anwenderspezifischen Gruppe "Umgebungskonfigurations-Administratoren" Berechtigungen gewähren, indem Sie diese Gruppe den ausgewählten Richtlinien hinzufügen und die erforderlichen Aktionen auswählen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich in CA EEM bei der CA Process Automation-Anwendung an.
2. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".
3. Gewähren Sie der ConfigAdmin-Gruppe die Anmeldung bei CA Process Automation und das Anzeigen der Startseite.
   a. Klicken Sie unter "Zugriffsrichtlinien" auf die Verknüpfung "Produktanwender".
   b. Klicken Sie auf die Anwenderanmeldungsrichtlinie "PAM40".
   c. Wählen Sie "Anwendungsgruppe" als Typ unter "Identitäten eingeben/suchen" aus, klicken Sie auf "Identitäten suchen", und klicken Sie auf "Suchen".
   d. Wählen Sie die anwenderspezifische Gruppe "ConfigAdmin" aus, und klicken Sie auf den Nach-unten-Pfeil.
   e. Wählen Sie "Console_Login" für die neue Identität aus.
   f. Klicken Sie auf "Speichern".
4. Gewähren Sie der ConfigAdmins-Gruppe die Berechtigungen, um eine Umgebung zu sperren und eine Aktion auszuführen, für die eine gesperrte Umgebung erforderlich ist.
   a. Klicken Sie unter "Zugriffsrichtlinien" auf die Verknüpfung "Umgebung".
   b. Klicken Sie in der Richtlinientabelle auf die Verknüpfung "PAM40 Umgebungsrichtlinie".
   c. Fügen Sie die Identitäten hinzu. Suchen Sie nach Gruppen. Geben Sie "Anwendungsgruppe" als Typ an, klicken Sie auf "Identitäten suchen", und klicken Sie auf "Suchen".
   d. Wählen Sie "ConfigAdmin" aus, und klicken Sie auf den Nach-unten-Pfeil.
   e. Wählen Sie die Berechtigung "Environment_Configuration_Admin" (Konfigurationsadministrator) aus.
   f. Klicken Sie auf "Speichern". Klicken Sie auf "Schließen".
5. Gewähren Sie der ConfigAdmin-Gruppe Berechtigungen, um auf die Registerkarte "Konfiguration" zuzugreifen und Koordinationsrechner und Agenten zu installieren.
   a. Klicken Sie auf "Konfigurationsbrowser".
   b. Klicken Sie auf "PAM40-Konfigurationsrichtlinie".

c. Suchen Sie nach "ConfigAdmin", und fügen Sie die Gruppe zu "Ausgewählte Identitäten" hinzu.

d. Wählen Sie "Client_Configuration_User" (Konfigurationsbrowser anzeigen) und "Configuration_Installations" aus.

6. Klicken Sie auf "Schließen".

Erstellen von Anwenderkonten für Umgebungskonfigurations-Administratoren

Sie können Anwenderkonten für einzelne Anwender erstellen, die die Rolle "Umgebungskonfigurations-Administrator" ausführen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Klicken Sie auf "Neuer Anwender".
4. Geben Sie die Anwender-ID als Namen ein.
5. Klicken Sie auf "Anwendungsanwenderdetails hinzufügen".
6. Wählen Sie die ConfigAdmin-Gruppe aus, und klicken Sie auf den rechten Pfeil.
7. Geben Sie bei Bedarf die globalen Anwenderdetails ein.
8. Geben Sie ein temporäres Kennwort in den Bereich "Authentifizierung" zweimal ein.
9. Klicken Sie auf "Speichern".
10. Wiederholen Sie diesen Vorgang für jeden Anwender in der Rolle "Umgebungskonfigurations-Administrator".

Erstellen der anwenderspezifischen ContentAdmin-Gruppe

Sie können in CA EEM eine anwenderspezifische Gruppe mit dem Namen "ContentAdmin" für Anwender in der Rolle "Umgebungsinhalts-Administrator" erstellen. Sie können diese Gruppe auf der standardmäßigen Designer-Gruppe basieren, um die Berechtigungen automatisch abzurufen, die der Designer-Gruppe zugewiesen sind.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich in CA EEM bei der CA Process Automation-Anwendung an.
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Klicken Sie auf "Gruppen".
4. Klicken Sie auf "Neue Anwendungsgruppe".
5. Geben Sie "ContentAdmin" als Namen der Gruppe und optional eine Beschreibung ein
6. Wählen Sie "Designer" unter "Verfügbare Benutzergruppen" aus, und klicken Sie auf den rechten Pfeil, um "Designer" in "Ausgewählte Benutzergruppen" zu verschieben.
7. Klicken Sie auf "Speichern".
8. Klicken Sie auf "Schließen".

Gewähren von Berechtigungen für die anwenderspezifische ContentAdmin-Gruppe

Sie können der anwenderspezifischen Gruppe "Umgebungsinhalts-Administratoren" Berechtigungen gewähren, indem Sie diese Gruppe zu Standardrichtlinien hinzufügen und die erforderlichen Berechtigungen auswählen. Viele der Richtlinienberechtigungen werden bereits der ContentAdmin-Gruppe gewährt, da Sie diese Gruppe auf der standardmäßigen Designer-Gruppe basiert haben. Sie fügen die Administratorrechte den Ordnern, Automatisierungsobjekten und Editoren auf der Registerkarte "Bibliothek" hinzu.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich in CA EEM bei der CA Process Automation-Anwendung an.
2. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".
3. Klicken Sie unter "Zugriffsrichtlinien" auf die Verknüpfung "Umgebung".
4. Klicken Sie in der Richtlinientabelle auf die Verknüpfung "PAM40 Umgebungsrichtlinie".
5. Fügen Sie die Identitäten hinzu. Suchen Sie nach Gruppen. Geben Sie "Anwendungsgruppe" als Typ an, klicken Sie auf "Identitäten suchen", und klicken Sie auf "Suchen".
6. Wählen Sie "ContentAdmin" aus, und klicken Sie auf den Nach-unten-Pfeil.
7. Wählen Sie die Berechtigungen "Environment_Library_Admin" (Inhaltsadministrator) aus.
8. Klicken Sie auf "Speichern".
9. Klicken Sie auf "Schließen".

Erstellen von Anwenderkonten für Umgebungsinhalts-Administratoren

Sie können Anwenderkonten für einzelne Anwender erstellen, die die Rolle "Umgebungsinhalts-Administrator" ausführen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an. (siehe Seite 46)
2. Klicken Sie auf die Registerkarte "Identitäten verwalten".
3. Klicken Sie auf "Neuer Anwender".
4. Geben Sie die Anwender-ID als Namen ein.
5. Klicken Sie auf "Anwendungsanwenderdetails hinzufügen".
6. Wählen Sie die ContentAdmin-Gruppe aus, und klicken Sie auf den rechten Pfeil.
7. Geben Sie bei Bedarf die globalen Anwenderdetails ein.
8. Geben Sie ein temporäres Kennwort in den Bereich "Authentifizierung" zweimal ein.
9. Klicken Sie auf "Speichern".
10. Wiederholen Sie diesen Vorgang für jeden Anwender in der Rolle "Umgebungsinhalts-Administrator".

Kontaktpunktsicherheit mit CA EEM

Der Zweck der Kontaktpunktsicherheit ist es, den Zugriff auf unternehmenskritischen Hosts oder Hosts mit streng vertraulichen Informationen auf eine Gruppe von hoch privilegierten Anwendern zu beschränken.

Dieser Abschnitt gilt nur, wenn Sie "Kontaktpunktsicherheit" für Kontaktpunkte in einer oder mehreren Umgebungen aktiviert haben.

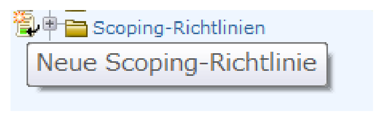
- Um zu bestimmen, ob "Kontaktpunktsicherheit" auf den Kontaktpunkten aktiviert ist, die dem Kandidatenhosts zugeordnet sind, überprüfen Sie in den Kontaktpunkteigenschaften die Konfiguration "Kontaktpunktsicherheit". Wenn "Von Umgebung übernehmen" markiert ist, sollten Sie in Betracht ziehen, die Konfiguration auf "Aktiviert" zu ändern.
- Um zu bestimmen, ob ein spezifischer schutzbedürftiger Kontaktpunkt, der einem Host zugeordnet ist, geschützt ist, überprüfen Sie die Filter in den Richtlinien zur Kontaktpunktsicherheit.

Gewähren des CA EEM-Zugriffs für Anwender zum Definieren von Richtlinien zur Kontaktpunktsicherheit

Standardmäßig kann sich nur der EiamAdmin-Anwender bei CA EEM anmelden. Wenn Sie einen richtlinienbasierten Ansatz zur Kontaktpunktsicherheit bereitstellen, können Sie bestimmte Anwender autorisieren, Richtlinien zur Kontaktpunktsicherheit in CA EEM zu erstellen. Autorisieren Sie die Inhaltsdesigner, die Prozesse mit Operatoren entwerfen, die auf Kontaktpunkten ausgeführt werden, die Hosts mit einem hohen Geschäftswert zugeordnet sind. Diese Kontaktpunkte können durch Richtlinien zur Kontaktpunktsicherheit geschützt werden, die die Anwender angeben, die zur Ausführung dieser Operatoren autorisiert sind.

So gewähren Sie angegebenen Richtlinien-Designern CA EEM-Zugriff und Autorisierungen für das Erstellen von Richtlinien mit der Ressourcenklasse "Kontaktpunktsicherheit"

1. Melden Sie sich in CA EEM bei der CA Process Automation-Anwendung an.
2. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".
3. Klicken Sie auf "Neue Scoping-Richtlinie".

4. Füllen Sie den Abschnitt "Allgemein" folgendermaßen aus:

   Name

   Gibt den Namen dieser Scoping-Richtlinie an. Zum Beispiel, Anwender, die Richtlinien zur Kontaktpunktsicherheit erstellen.

   Beschreibung

   (Optional) Geben Sie eine kurze Beschreibung an. Zum Beispiel: Ermöglicht es angegebenen Anwendern, anwenderspezifische Richtlinien nur mit der Ressourcenklasse "Kontaktpunktsicherheit" zu erstellen.

   Kalender und Name der Ressourcenklassen

   Überspringen Sie die Kalenderoption und akzeptieren Sie den Standardeintrag "SafeObject" für "Name der Ressourcenklasse".

   Typ

   Geben Sie eine Zugriffssteuerungsliste an

   Hinweis: Eine Meldung wird angezeigt, die darauf hinweist, dass das Ändern von Richtlinientypen einige Filter zurücksetzt. Klicken Sie auf "OK".

5. Fügen Sie für Identitäten die Namen aller Anwender hinzu, die Prozesse entwerfen, die sich auf Kontaktpunktsicherheit beziehen. Den zu dieser Richtlinie hinzugefügten Anwendern wird Anmeldezugriff auf CA EEM und das Erstellen von Richtlinien zur Kontaktpunktsicherheit gewährt. Eine Richtlinie zur Kontaktpunktsicherheit gibt die Anwender an, die zur Ausführung der Operatoren von einer bestimmten Operatorkategorie auf einem angegebenen Kontaktpunkt autorisiert werden sollen.

   Hinweis: Wenn Sie diese Richtlinie testen möchten, erstellen Sie einen Anwender mit der Standardanwendergruppe, und fügen Sie hier diesen Anwendernamen hinzu. Nachdem Sie diese Richtlinie gespeichert haben, melden Sie sich mit Ihrem Testanwendernamen bei CA EEM an. Beachten Sie, dass Sie in CA EEM lediglich eine Richtlinie mit der Ressourcenklasse "Kontaktpunkt" erstellen können.

   a. Akzeptieren Sie "Anwender" als Typ oder wählen Sie einen anderen Wert aus.

   b. Klicken Sie auf die Verknüpfung "Identitäten suchen".

   c. Geben Sie Suchkriterien ein, die den geplanten Anwender oder Gruppe enthalten, und klicken Sie auf "Suchen".

   d. Wählen Sie einen Anwender oder Gruppe aus der angezeigten Liste der verfügbaren Identitäten aus, und klicken Sie auf den rechten Pfeil.

      Der ausgewählte Anwender oder die ausgewählte Gruppe wird in der Liste "Ausgewählte Identitäten" angezeigt.

   e. Wiederholen Sie diesen Vorgang für jeden Anwender, den Sie zum Erstellen von Richtlinien zur Kontaktpunktsicherheit autorisieren möchten.

6. Konfigurieren Sie folgendermaßen die Zugriffssteuerungsliste:

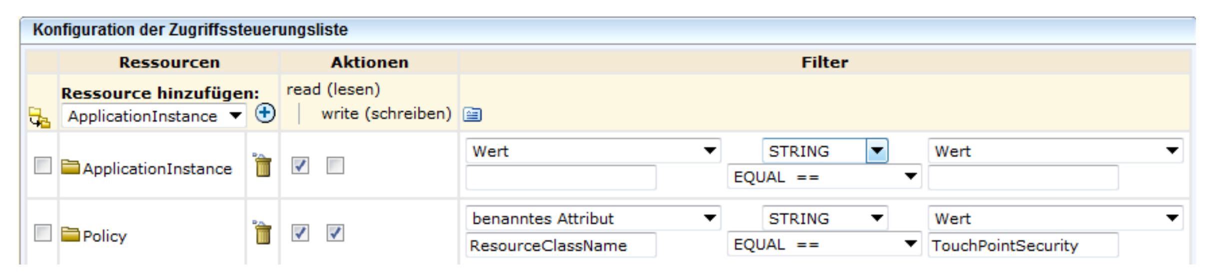
   a. Wählen Sie folgende Ressourcen aus der Drop-down-Liste aus, und klicken Sie auf "Hinzufügen", um sie der Liste hinzuzufügen.

      - ApplicationInstance
      - Richtlinie
      - Anwender
      - GlobalUser
      - UserGroup
      - GlobalUserGroup

   b. Klicken Sie für alle Ressourcen auf "lesen". Klicken Sie für Richtlinien auf "schreiben".

   c. Klicke Sie auf "Filter".

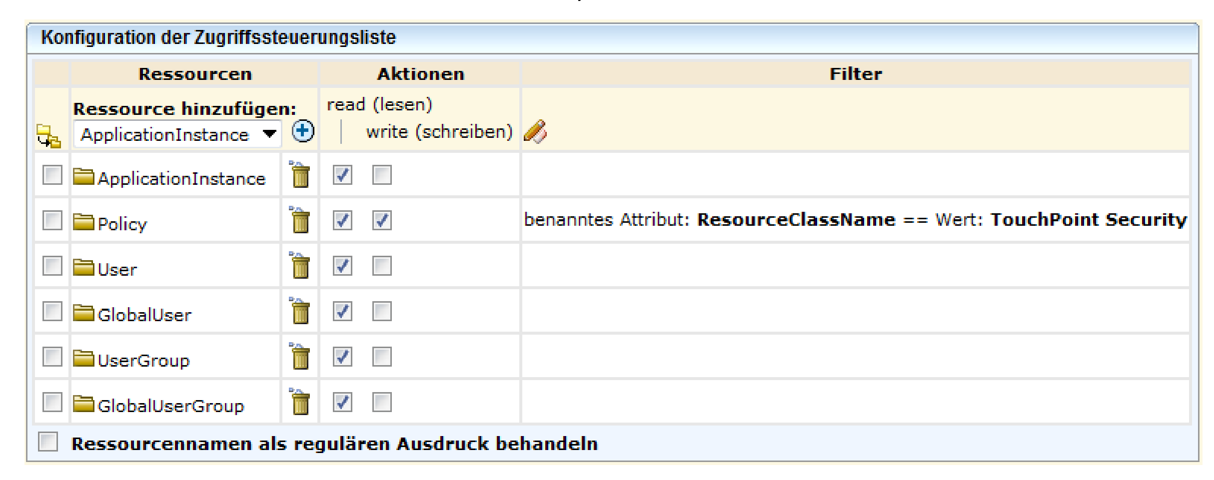
   d. Wählen Sie für "Richtlinie" das benannte Attribut aus der ersten Drop-down-Liste aus. Geben Sie im Feld unter "benanntes Attribut" den Wert "RessourceKlassenName" ein. Geben Sie im Wertfeld nach "EQUAL" den Wert "TouchPointSecurity" ein. Geben Sie kein Leerzeichen zwischen "TouchPoint" und "Security" ein.



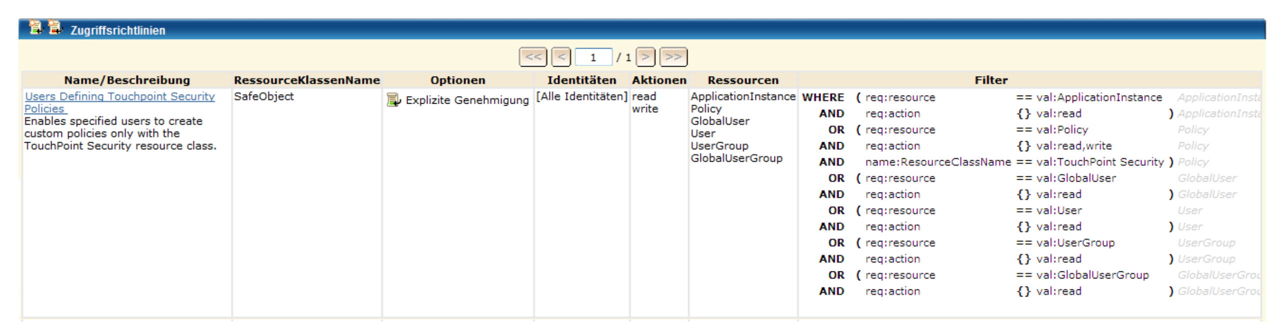
   e. Lassen Sie die restlichen Felder auf der Filterseite so, wie sie sind.

7. Klicken Sie auf "Speichern".

8. Stellen Sie sicher, dass "Konfiguration der Zugriffssteuerungsliste" mit dem folgenden Beispiel genau übereinstimmt. Das System fügt ein Leerzeichen zwischen "TouchPoint" und "Security" hinzu.



9. Überprüfen Sie, ob Ihre Richtlinie dem folgenden Beispiel ähnelt: Im Beispiel zeigen die fehlenden Spalten an, dass "RessourceKlassenName" "SafeObject" ist, der Optionswert ist "Explizite Genehmigungen" und "Identitäten" ist Ihre Liste der Anwender. Dies sind Anwender, die Prozesse für Kontaktpunktsicherheit entwerfen und eine zugeordnete Richtlinie erstellen.



Informationen zur Kontaktpunktsicherheit

Kontaktpunktsicherheit ermöglicht es Ihnen, Kontaktpunkte zu sichern, die unternehmenskritischen Hosts und Hosts mit vertraulichen Daten zugeordnet sind. Sie können solche Kontaktpunkte vor nicht autorisiertem Zugriff schützen. Sie können Richtlinien für Kontaktpunkt erstellen, die ausgewählte Anwender oder eine hoch privilegierte Gruppe als einzige Identitäten angeben, die einen Operator auf diesem Ziel ausführen können. Richtlinien geben Identitäten an, die zur Ausführung bestimmter Operatoren auf angegebenen Kontaktpunkten autorisiert sind. Die Operatoren, die Programme und Skripte ausführen, sind in angegebenen Operatorkategorien enthalten.

Zusammenfassend: Mit den CA EEM-Richtlinien zur Kontaktpunktsicherheit werden die angegebenen Identitäten zur Ausführung von Skripten in Operatoren von angegebenen Kategorien auf angegebenen Kontaktpunkten in einer angegebenen Umgebung autorisiert.

Sehen Sie sich den folgenden Beispielausschnitt einer einfachen Richtlinie zur Kontaktpunktsicherheit an.

Identitäten	Aktionen	Ressourcen	Filter
ug:High-PrivilegedUsers	[All Actions]	✓ Regex Compare Network Utilities Module Process Module File* Module	**WHERE** (name:Environment == val:Production **AND** (name:Touchpoint == val:SensitiveHostTP1 **OR** name:Touchpoint == val:SensitiveHostTP2 **OR** name:Touchpoint == val:SensitiveHostTP3))

Das Beispiel ist ein Teil einer Richtlinie. Die Richtlinie erlaubt es nur den Anwender der Gruppe "High-PrivilegedUsers", Operatoren von angegebenen Kategorien auf angegebenen Kontaktpunkten in der Produktionsumgebung auszuführen. Die Beispielkontaktpunkte haben den Namen "SensitiveHostTP1", "SensitiveHostTP2" und "SensitiveHostTP3". Die angegebenen Zugriffssteuerungslisten-IDs schließen das Netzwerkhilfsprogramm-Modul und das Prozessmodul (für Befehlsausführung) ein. Dateimodul schließt sowohl Dateimodul für Dateiverwaltung als auch das Dateiübertragungsmodul ein.

Hinweis: Weitere Informationen finden Sie unter Identifizieren der Zugriffssteuerungslisten-IDs zum Hinzufügen als Ressourcen (siehe Seite 137).

Ein Prozess mit einem Operatorziel, das von einer Richtlinie zur Kontaktpunktsicherheit geschützt ist, kann nur erfolgreich sein, wenn ein autorisierter Anwender ihn ausführt. Der Anwender, unter dem der Prozess ausgeführt wird, ist in der Richtlinie als Identität angegeben. Die Richtlinie identifiziert Anwender nach Namen oder Gruppenmitgliedschaft, Operatoren nach Zugriffssteuerungslisten-IDs, die Quellenkategorien zugeordnet sind, und Kontaktpunkte nach Namen und/oder nach Umgebung.

Richtlinien zur Kontaktpunktsicherheit sichert den Zugriff auf individuelle Zielhosts, indem kontrolliert wird, wer Operatoren auf einem bestimmten Kontaktpunkt oder auf einer bestimmten Hostgruppe ausführt. Eine Prozessinstanz wird im Namen eines Anwenders ausgeführt. Wenn der Prozess einen Operator auf einem Kontaktpunkt oder in einer Hostgruppe ausführt, die in der CA EEM-Richtlinie zur Kontaktpunktsicherheit angegeben ist, versucht CA EEM, diesen Anwender zu autorisieren. CA EEM überprüft, ob der Anwender als Identität in einer Richtlinie zur Kontaktpunktsicherheit für diesen Kontaktpunkt angegeben ist. Wenn die Prozessinstanz im Namen eines nicht autorisierten Anwenders ausgeführt wird, dann schlägt der Operator fehl.

Sie geben empfindliche Hosts als Kontaktpunkte, Proxy-Kontaktpunkte oder Hostgruppen an.

Sie können den Zugriff auf angegebene Hosts auf hoch privilegierte Anwender beschränken. Sie können einem angegebenen Anwender oder einer Gruppe Zugriff gewähren, dem bzw. der der folgende erforderliche Zugriff erteilt wurde:

- Gewährt Aktion Console_Login (Anwender) in der Anwenderanmeldungsrichtlinie "PAM40".
- Gewährt Aktion Environment_Library_User (Anwender) in der Umgebungsrichtlinie "PAM40".

Anwendungsfälle: Wann ist Kontaktpunktsicherheit erforderlich?

Kontaktpunktsicherheit wird in den folgenden Fällen benötigt:

- Ein Host in Ihrer Umgebung, das ein Operatorziel sein kann, enthält vertrauliche Informationen, wie z. B. Sozialversicherungsnummer, Kreditkartennummer oder gesundheitliche Daten. Sie sollten den Zugriff auf diesen vertraulichen Prozess auf eine einzelne Person oder auf eine kleine und hoch privilegierte Gruppe beschränken.

  Das Ziel kann einer der folgenden Hosts sein:

  - Der Host mit einem Agenten, der einem Kontaktpunkt zugeordnet ist.
  - Der Host mit einem Agenten, der einem Proxy-Kontaktpunkt, der über eine SSH-Verbindung zu einem Remote-Host verfügt, zugeordnet ist.
  - Der Host mit einem Agenten, der einer Hostgruppe zugeordnet ist, die sich auf Remote-Hosts bezieht und über eine Verbindung zu Remote-Hosts verfügt.

- Wenn Sie einen Agenten auf einem Host als Root-Anwender (UNIX), Administrator (Windows) oder als Anwender mit bestimmten Rechten ausführen. Nehmen Sie an, Sie müssten alle Skripte und Programme auf diesem Agenten unter der gleichen Identität wie den Agenten selbst ausführen. Das heißt, Sie möchten nicht zu einem anderen Anwender wechseln, der Anmeldeinformationen benötigt. Um ein Sicherheitsrisiko zu verhindern, können Sie festlegen, dass Anwender mit eingeschränkten Berechtigungen keine Skripte unter der gleichen Identität wie der Agent, z. B. der Root-Anwender, ausführen dürfen.

- Wenn Sie Hostgruppen nutzen, die standardmäßige Anmeldeinformationen für Betriebssysteme definieren, um Befehlsausführungsoperatoren auf gesamten Subnetzen auszuführen. Nehmen Sie an, Sie müssten alle Skripte und Programme auf dieser Hostgruppe mithilfe der Anmeldeinformationen des Betriebssystems ausführen. Sie müssen ein Sicherheitsrisiko verhindern, indem Sie nicht erlauben, dass Anwender mit eingeschränkten Berechtigungen Skripte mithilfe von Anmeldeinformationen für Betriebssysteme erstellen und ausführen.

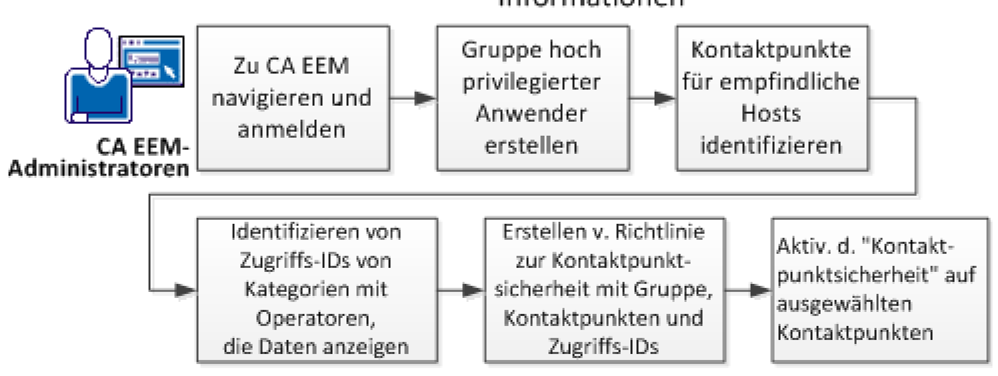
- Anwender, die einen Prozess ausführen, können zur Laufzeit Operatorziele für Operatoren auswählen, die über eine Variable im Zielfeld verfügen. Ein Operatorziel ist normalerweise ein Kontaktpunkt. Es kann aber auch ein Proxy-Kontaktpunkt, ein FQDN oder eine IP-Adresse sein, auf die über eine Hostgruppe verwiesen wird. Dieses flexible Design ermöglicht es einem beliebigen Anwender, der zur Ausführung des Prozesses autorisiert ist, ein Ziel zur Laufzeit auszuwählen.

  Ein Sicherheitsproblem tritt auf, wenn ein verfügbarer Kontaktpunkt Zugriffbeschränkungen benötigt. Stellen Sie sich vor, dass ein Operator erfolgreich auf zwei unterschiedlichen Kontaktpunkten ausgeführt wird, von denen jeder eine Service Desk-Anwendung darstellt. Ein Kontaktpunkt stellt einen Service Desk für den allgemeinen Zugriff dar, während der andere Kontaktpunkt nur für Administratoren entworfen wurde. Kontaktpunktsicherheit stellt sicher, dass nur Administratoren diesen Beispieloperator auf dem Kontaktpunkt, der für Administratoren entworfen wurde, ausführen können. Richtlinien zur Kontaktpunktsicherheit in CA EEM beschränken den Zugriff.

Kontaktpunktsicherheit ist auch für Prozessdesigner nützlich. Während der Prozessentwicklung installieren verschiedene Designer einen Agenten auf ihren persönlichen Hosts und erstellen Kontaktpunkte für ihre Agenten. Sie möchten normalerweise nicht, dass andere Anwender Operatoren auf ihren lokalen Hosts ausführen. Kontaktpunktsicherheit bietet diesen Schutz. Wenn "Kontaktpunktsicherheit" aktiviert ist, wird die Autorisierung zur Ausführung der Operatoren auf dem ausgewählten Ziel zur Laufzeit überprüft. Das Durchsetzen der Richtlinien stellt sicher, dass Anwender, die einen Prozess ausführen, nur Operatoren auf Kontaktpunkten ausführen können, für die sie autorisiert sind.

Beschränken des Zugriffs auf Hosts mit vertraulichen Informationen

"Kontaktpunktsicherheit" erfüllt den Bedarf, den Zugriff auf unternehmenskritische Hosts oder Hosts mit streng vertraulichen Informationen zu beschränken. Folgende Abbildung schlägt eine Vorgehensweise vor, um dieses Sicherheitsziel zu erfüllen.



Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Erstellen Sie eine Gruppe mit hoch privilegierten Anwendern.

   Weitere Informationen finden Sie unter Erstellen der anwenderspezifischen ContentAdmin-Gruppe (siehe Seite 124).
3. Identifizieren Sie die Kontaktpunkte, die empfindlichen Hosts zugeordnet sind.

   Weitere Informationen finden Sie unter Anzeigen der Kontaktpunkte und Hostgruppen für einen ausgewählten Agenten (siehe Seite 223).
4. Identifizieren Sie die Kategorien mit Operatoren, die Daten darstellen.
5. Identifizieren Sie dann die Zugriffssteuerungslisten-IDs, die den Kategorien zugeordnet sind.
   - Weitere Informationen zu den in Frage kommenden Zugriffssteuerungslisten-IDs finden Sie unter Beispiel: Sichern von kritischen Kontaktpunkten (siehe Seite 140).
   - Beschreibungen von allen Kategorien finden Sie im Abschnitt Operatorkategorien und wo Operatoren ausgeführt werden (siehe Seite 333).
   - Weitere Informationen zu Operatorbeschreibungen finden Sie im *Referenzhandbuch für Inhaltsdesign*.
6. Erstellen Sie eine Richtlinie zur Kontaktpunktsicherheit mit dieser Gruppe sowie mit diesen Kategorien und Kontaktpunkten.

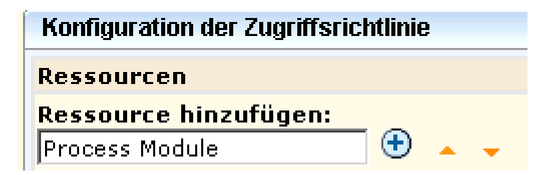
   Weitere Informationen finden Sie unter Erstellen einer Richtlinie der Kontaktpunktsicherheit (siehe Seite 138).
7. Aktivieren Sie "Kontaktpunktsicherheit" auf ausgewählten Kontaktpunkten.
   - Weitere Informationen finden Sie unter Konfigurieren von Kontaktpunkteigenschaften (siehe Seite 238).
   - Weitere Informationen finden Sie unter Konfigurieren von Proxy-Kontaktpunkteigenschaften (siehe Seite 262).
   - Weitere Informationen finden Sie unter Konfigurieren von Hostgruppeneigenschaften (siehe Seite 270).

Weitere Informationen:

Ansatz beim Konfigurieren der Kontaktpunktsicherheit (siehe Seite 160)

Identifizieren der Zugriffssteuerungslisten-IDs zum Hinzufügen als Ressourcen

Wenn Sie eine Richtlinie zur Kontaktpunktsicherheit erstellen, identifizieren Sie nicht direkt die Operatoren zum Bearbeiten von Kontaktpunkten, die Sie sichern möchten. Sie identifizieren stattdessen die Kategorien, zu denen diese Operatoren gehören. Sie identifizieren die Kategorien nicht nach Namen, sondern nach ihren Zugriffssteuerungslisten-IDs.

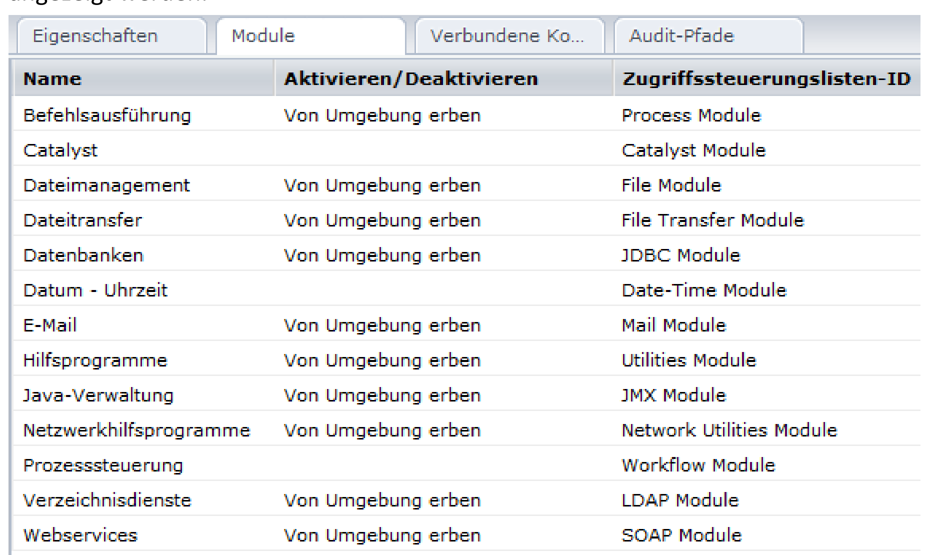


Nicht alle Kategorien enthalten Operatoren, die die Sicherheit eines Hosts mit vertraulichen Informationen gefährden könnten. Schätzen Sie die Auswirkung der Operatoren ein, bevor Sie Ressourcen hinzufügen.

Sie können die Zugriffssteuerungslisten-ID identifizieren, die als Ressource zu einer Richtlinie der Kontaktpunktsicherheit hinzugefügt werden soll.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA Process Automation, und melden Sie sich an (siehe Seite 18).
2. Klicken Sie auf die Registerkarte Konfiguration.
3. Wählen Sie einen Agenten aus dem Knoten Agenten aus, und wählen Sie die Registerkarte Module aus.
4. Notieren Sie auf die Namen, die in der Spalte "Zugriffssteuerungslisten-ID" angezeigt werden.



Name	Aktivieren/Deaktivieren	Zugriffssteuerungslisten-ID
Befehlsausführung	Von Umgebung erben	Process Module
Catalyst		Catalyst Module
Dateimanagement	Von Umgebung erben	File Module
Dateitransfer	Von Umgebung erben	File Transfer Module
Datenbanken	Von Umgebung erben	JDBC Module
Datum - Uhrzeit		Date-Time Module
E-Mail	Von Umgebung erben	Mail Module
Hilfsprogramme	Von Umgebung erben	Utilities Module
Java-Verwaltung	Von Umgebung erben	JMX Module
Netzwerkhilfsprogramme	Von Umgebung erben	Network Utilities Module
Prozesssteuerung		Workflow Module
Verzeichnisdienste	Von Umgebung erben	LDAP Module
Webservices	Von Umgebung erben	SOAP Module

Wichtig! Die Spalte "Zugriffssteuerungslisten-ID" listet Modulnamen auf. Verwenden Sie diese Liste als Referenz, wenn Sie ausgewählte Modulnamen in das Feld "Ressourcen" in einer Richtlinie zur Kontaktpunktsicherheit eingeben.

Erstellen einer Richtlinie der Kontaktpunktsicherheit

Bei der Ausführung eines Prozesses werden bestimmte Operatoren auf angegebenen Zielen in einer angegebenen Reihenfolge ausgeführt. Eine anwenderspezifische Richtlinie zur Kontaktpunktsicherheit gewährt angegebenen Anwendern oder Gruppen die Berechtigung zur Ausführung von angegebenen Operatoren auf angegebenen Zielen. Die CA EEM-Administratoren können Richtlinien für die Kontaktpunktsicherheit erstellen.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte Zugriffsrichtlinien verwalten.
3. Klicken Sie unter Zugriffsrichtlinien für Kontaktpunktsicherheit auf die Schaltfläche Neue Zugriffsrichtlinie.
4. Geben Sie im Formular für die neue Zugriffsrichtlinie für die Ressourcenklasse "Kontaktpunktsicherheit" einen Namen für die anwenderspezifische Richtlinie für Kontaktpunktsicherheit ein.

   Im Abschnitt Identitäten eingeben/suchen können Sie den Zielanwender oder die Zielgruppe angeben.
5. Wählen Sie den Typ des Ziels aus, auf das Zugriff erteilt werden soll:
   - Wählen Sie Benutzer aus, wenn das Ziel ein globaler Benutzer ist.
   - Wählen Sie Globale Gruppe aus, wenn das Ziel eine Gruppe aus einem referenzierten Anwenderspeicher ist.
   - Wählen Sie Anwendungsgruppe aus, wenn das Ziel eine von Ihnen definierte anwenderspezifische Gruppe oder eine standardmäßige Gruppe ist.
6. Klicken Sie auf Identitäten suchen.
7. Wählen Sie die Identitäten aus, für die diese Richtlinie gilt, und klicken Sie auf den Nach-unten-Pfeil.

   Die Liste Ausgewählte Identitäten zeigt Ihre Auswahl an.
8. Wählen Sie die Aktion Ausführen aus.

9. Geben Sie im Feld Ressource hinzufügen die Zugriffssteuerungslisten-ID der Quelloperator-Kategorie ein, die die Operatoren enthalten, für die diese Richtlinie gilt. Zum Beispiel:
   - Tippen Sie für die Operatorkategorie "Befehlsausführung" **Process Module**.
   - Tippen Sie für die Operatorkategorie "Dateimanagement" **File Module**.
   - Tippen Sie für die Operatorkategorie "Dateitransfer" **File Transfer Module**.
   - Tippen Sie für die Operatorkategorie "Netzwerkhilfsprogramme" **Network Utilities Modul**.

   Sie können reguläre Ausdrücke eingeben, um die entsprechenden Operatorkategorien einzuschließen. Wählen Sie dann "Ressourcennamen als regulären Ausdruck behandeln" aus. Zum Beispiel deckt die Eingabe "File*" Operatoren in den Kategorien "Dateimanagement" (File Management) und "Dateitransfer" (File Transfer) ab.
10. Klicken Sie auf Hinzufügen.
11. Fügen Sie einen Filter hinzu, der die Umgebung angibt, die die Richtlinienziele enthält:
    - Legen Sie das benannte Attribut auf Umgebung fest.
    - Legen Sie den Operator "STRING" auf EQUAL fest.
    - Legen Sie den Wert auf den *Umgebungsnamen* fest.
12. Fügen Sie weitere Filter hinzu, die die Ziele nach Kontaktpunktnamen angeben:
    - Legen Sie das benannte Attribut auf Kontaktpunkt fest.
    - Legen Sie den Operator "STRING" auf EQUAL fest.
    - Legen Sie den Wert auf den *Kontaktpunktnamen* fest.
13. Klicken Sie auf "Speichern".

    Wenn die Richtlinien für Kontaktpunktsicherheit so konfiguriert sind, dass sie durchgesetzt werden müssen, wertet das Produkt die Richtlinie aus und setzt sie durch.

Beispiel: Sichern von kritischen Kontaktpunkten

Die Kontaktpunktsicherheit stellt sicher, dass die Möglichkeit zur Ausführung der Operatoren auf unternehmenskritischen Hosts auf kleine Gruppe mit hoch privilegierten Anwendern beschränkt ist. Empfindliche Hosts können am besten geschützt werden, indem eine Richtlinie der Kontaktpunktsicherheit erstellt wird und alle zugeordneten Kontaktpunkte in einem Filter aufgelistet werden. Aktivieren Sie dann "Kontaktpunktsicherheit" in der Eigenschaftseinstellung für jeden dieser Kontaktpunkte.

Beispiel: Konfiguration der Kontaktpunktsicherheit für einen kritischen Kontaktpunkt

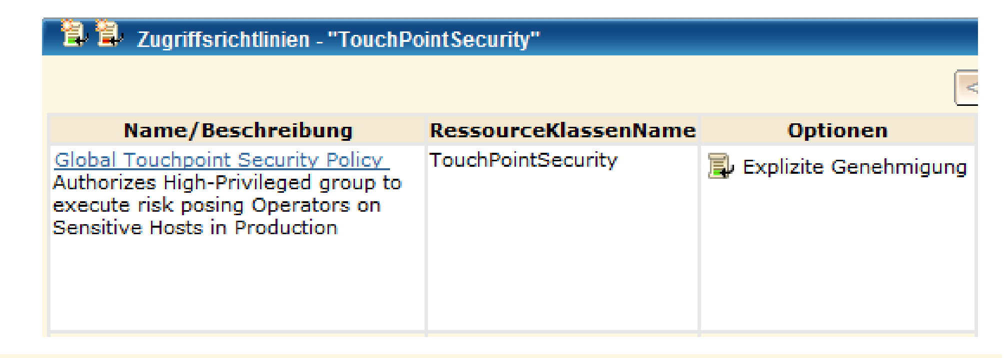
Das folgende Beispiel zeigt die Eigenschaften eines ausgewählten Kontaktpunkts. Wenn Kontaktpunktsicherheit aktiviert ist, wird jeder Versuch, einen Operator auf diesem Kontaktpunkt auszuführen, anhand der Richtlinien zur Kontaktpunktsicherheit überprüft.



Beispiel: Richtlinie zur Kontaktpunktsicherheit für kritische Kontaktpunkte

Erstellen Sie eine Richtlinie zur Kontaktpunktsicherheit, um sicherzustellen, dass nur hoch privilegierte Anwender Operatoren auf empfindlichen Hosts in Ihrer Produktionsumgebung ausführen. Fügen Sie in der Richtlinie zur Kontaktpunktsicherheit die Zugriffssteuerungslisten-ID hinzu, die jeder Kategorie zugeordnet ist, die Operatoren enthält, die ein Risiko darstellen könnten. Fügen Sie einen Filter für Ihre Umgebung hinzu. Fügen Sie einen Filter für jeden Kontaktpunkt hinzu, der auf empfindliche Hosts verweist.

Beachten Sie das folgende Beispiel für eine globale Richtlinie zur Kontaktpunktsicherheit. Die Beispielrichtlinie gewährt der Gruppe mit hoch privilegierten Anwendern die Ausführung von Skripten oder Programmen mithilfe von Operatoren in fünf Kategorien auf Kontaktpunkten mit hohem Risiko. Zugriffssteuerungslisten-IDs stellen die fünf Kategorien dar. Diese Richtlinie gilt nur für die angegebenen Kontaktpunkte in der Produktionsumgebung.



Name/Beschreibung	RessourceKlassenName	Optionen
Global Touchpoint Security Policy Authorizes High-Privileged group to execute risk posing Operators on Sensitive Hosts in Production	TouchPointSecurity	Explizite Genehmigung

Identitäten	Aktionen	Ressourcen	Filter
ug:High-PrivilegeUsers	Execute	Process Module File Module File Transfer Module JMX Module Network Utilities Module	**WHERE** name:ENVIRONMENT == val:Production **AND** name:TOUCHPOINT == val:TP-SensitiveHost1 **OR** name:TOUCHPOINT == val:TP-SensitiveHost2 **OR** name:TOUCHPOINT == val:TP-SensitiveHost3 **OR** name:TOUCHPOINT == val:TP-SensitiveHost4 **OR** name:TOUCHPOINT == val:TP-SensitiveHostn

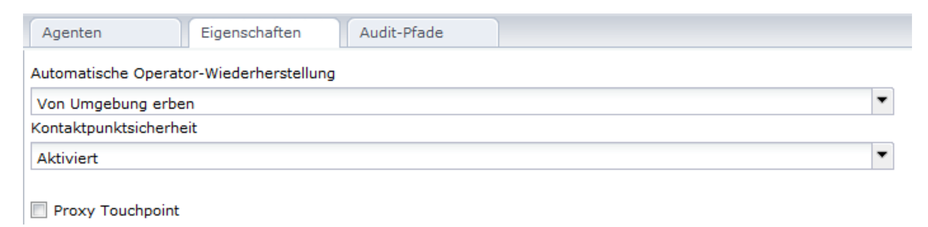
Beispiel: Sichern des Kontaktpunkts für meinen Host

Nehmen Sie an, dass Sie einen Agenten auf Ihrem Host installieren, und Sie möchten nicht, dass jemand außer Ihnen Operatoren auf Ihrem Host ausführen kann. Um Kontaktpunktsicherheit zum Schutz eines kritischen Hosts zu verwenden, sollten Sie in Betracht ziehen, die erforderlichen Aufgaben in folgender Reihenfolge auszuführen.

1. Installieren Sie einen Agenten auf dem Host.
2. Ordnen Sie einen Kontaktpunkt in einer angegebenen Umgebung mit diesem Host zu.
3. Erstellen Sie eine Richtlinie zur Kontaktpunktsicherheit, die Sie als "Identität" auflistet. Fügen Sie die Zugriffssteuerungslisten-ID für jede Kategorie mit Operatoren hinzu, die auf Kontaktpunkten, die Agenten zugeordnet sind, ausgeführt werden können.
4. Aktivieren Sie "Kontaktpunktsicherheit" in den Kontaktpunkteigenschaften für diesen Host.

Beispiel: Aktivieren der Kontaktpunktsicherheit auf dem Kontaktpunkt "My PC"

Der Parameter "Kontaktpunktsicherheit" für den ausgewählten Kontaktpunkt "MyPC-TP" wird auf "Aktiviert" eingestellt.



Beispiel: Erstellen einer Richtlinie zur Kontaktpunktsicherheit, die nur mir erlaubt, Operatoren auf dem Kontaktpunkt "My PC" auszuführen

Nehmen Sie im folgenden Beispiel an, dass der geschützte Host einem Anwender mit dem Namen "MyPCowner" gehört. Beachten Sie, dass "MyPCowner" die einzige Identität ist, die zur Ausführung von Operatoren auf dem Kontaktpunkt "MyPC-TP" autorisiert ist. Hier sind die Zugriffssteuerungslisten-IDs allen Kategorien mit Operatoren zugeordnet, die auf einem Agentenhost ausgeführt werden können. In diesem Fall schließen die Referenzen Kategorien von Operatoren ein, die keine Änderungen am Host vornehmen. Der Grundgedanke in diesem Beispiel ist, dass der Anwender nicht möchte, dass externe Anwender auf den Host, der dem Kontaktpunkt "MyPC-TP" zugeordnet ist, zugreifen. Nur "MyPCowner" kann Prozesse auf "MyPC-TP" ausführen, wenn Kontaktpunktsicherheit aktiviert ist.



Name/Beschreibung	RessourceKlassenName	Optionen
Secure_TP_My_PC_	TouchPointSecurity	Explizite Genehmigung

Der Kontaktpunktname wird als Wert im Filter angegeben.

Identitäten	Aktionen	Ressourcen	Filter
MyPCowner	Execute	Process Module JDBC Module LDAP Module Mail Module File Module File Transfer Module JMX Module Network Utilities Module Utilities Module SOAP Module	**WHERE** name:ENVIRONMENT == val:Test **AND** name:TOUCHPOINT == val:MyPC-TP

Autorisieren der Laufzeitaktionen mit CA EEM

CA Process Automation gibt eine präzise abgestimmte Zugriffssteuerung für Vorgänge und Anwenderaktionen auf bestimmte Automatisierungsobjekte an, wie z. B. Prozesse, Datensätze, Kalender und Ablaufpläne. Die Steuerung umfasst herkömmliche Lese- und Schreibrechte sowie Rechte, um einen Prozess zu starten und die Instanzen zu überwachen. Zugriffsrechte werden in allen externen Schnittstellen durchgesetzt, einschließlich der CA Process Automation-Anwenderoberfläche und der Webservices. Außerdem bietet CA Process Automation die Möglichkeit, Vorgänge auf Zielhosts zu sichern, sodass nur autorisierte Anwender sie ausführen können.

Um die Anwender zu beschränken, die eine der folgenden Laufzeitaktionen ausführen können, erstellen Sie eine CA EEM-Richtlinie, und geben Sie die Anwender oder Gruppen an, die autorisiert werden sollen.

- Führen Sie Skripte oder Programme innerhalb Operatoren aus, die von angegebenen Kategorien, die auf angegebene Kontaktpunkte in einer angegebenen Umgebung abzielen, abgeleitet sind.
- Steuern Sie einen Ablaufplan, einschließlich Aktivieren und Deaktivieren des Ablaufplans.
- Untersuchen oder ändern Sie einen Datensatz.
- Steuern Sie eine Prozessinstanz, einschließlich Unterbrechen, Neustarten, Fortfahren oder Abbrechen einer Prozessinstanz.
- Steuern einer Ressource, einschließlich Sperren, Entsperren, Übernehmen, Zurückgeben oder Hinzufügen einer Variablen zu einer Ressource. Hinzufügen oder Entfernen einer Ressourceneinheit.
- Entfernen Sie ein Startauftragsformular aus der Warteschlange oder starten Sie es.

Zusätzlich können Sie eine Richtlinie erstellen, die Lese- und Schreibrechte auf einem anderen Automatisierungsobjekt autorisiert.

Ändern der Eigentümer für Automatisierungsobjekte

Der Anwender, der ein Automatisierungsobjekt oder einen Ordner erstellt, ist standardmäßig der Verantwortliche. Der Verantwortliche hat die volle Kontrolle über das Automatisierungsobjekt oder den Ordner. Ein Verantwortlicher kann den Besitz auf einen anderen CA Process Automation-Anwender übertragen.

Hinweis: Die Berechtigung "CA EEM-Environment_Content_Administrator" gewährt die vollständige Kontrolle über alle Automatisierungsobjekte und Ordner. Alle Administratoren, die zur PAMAdmins-Gruppe gehören, haben diese Berechtigung.

Wenn Sie "Laufzeitsicherheit" aktivieren, dann kann nur der Verantwortliche des Prozesses (oder ein Administrator) diesen Prozess starten.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Wählen Sie ein oder mehrere Objekte einschließlich Ordner aus.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche "Verantwortlichen festlegen".
4. Wählen Sie in der Liste "Verfügbare Anwender" das Anwenderkonto aus, das als neuer Verantwortlicher eingerichtet werden soll. Verwenden Sie die Suche, um übereinstimmende Anwenderkonten zu finden.
5. Klicken Sie auf Speichern und Schließen.

Kapitel 5: Verwalten der CA Process Automation-Domäne

In CA Process Automation umfasst die Domäne das gesamte System. Die Domänenverwaltung schließt alle Aufgaben ein, die ausschließlich von einem Administrator mit Domänenadministratorrechten durchgeführt werden. Zu den Aufgaben gehören das Hinzufügen von Umgebungen, das gebündelte Entfernen von nicht verwendeten Agenten und Kontaktpunkten und die Konfiguration von Sicherheit, Eigenschaften, Operatorkategorien und Auslösern auf der Domänenebene. In diesem Kapitel wird nur auf die Aufgaben eingegangen, die beim ersten Setup eines neu installierten CA Process Automation-Systems durchgeführt werden. In den nachfolgenden Kapiteln werden Aufgaben behandelt, die normalerweise bei der Entwicklung von Inhalten ausgeführt werden.

Dieses Kapitel enthält folgende Themen:

Sperren der Domäne

Administratoren können die Domäne sperren. Eine Sperre schützt die Domäne vor gleichzeitigen Aktualisierungen durch mehrere Anwender. Bevor Sie eine Konfigurationsänderung auf Domänenebene vornehmen, sperren Sie die Domäne.

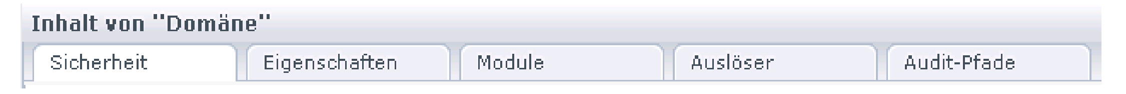
Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Wählen Sie "Domäne" im Auswahlmenü "Konfigurationsbrowser" aus, und klicken Sie auf "Sperren".

Wenn Sie die Konfigurationsänderungen abgeschlossen haben, wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren der Inhalte der Domäne

Wenn Sie "Domäne" im Konfigurationsbrowser auswählen, werden folgende Registerkarten unter "Inhalte" von "Domäne" angezeigt:



- Sicherheit

  Weitere Informationen finden Sie unter Konfigurieren von CA EEM-Sicherheitseinstellungen für die Domäne (siehe Seite 150).

- Eigenschaften

  Weitere Informationen finden Sie unter Konfigurieren von Domäneneigenschaften (siehe Seite 156).

- Module

  Weitere Informationen finden Sie unter Konfigurieren der Operatorkategorien (siehe Seite 289). Nach diesem Thema wird der Konfigurationsvorgang für jede Operatorkategorie behandelt. Vor jedem Konfigurationsvorgang finden Sie eine Beschreibung der Kategorien.

- Auslöser

  Weitere Informationen finden Sie unter Konfigurieren und Verwenden von Auslösern (siehe Seite 336). Nach diesem Thema werden Konfigurationsdetails für jeden Auslösertyp behandelt.

- Audit-Pfade

  Weitere Informationen finden Sie unter Anzeigen des Audit-Pfads für die Domäne (siehe Seite 359).

Weitere Informationen:

Verwalten der Domäne (siehe Seite 415)

Info zur Konfigurationsvererbung

Die Konfiguration auf Domänenebene umfasst die folgenden Einstellungstypen:

- Sicherheit
- Eigenschaften
- Operatorkategorien
- Auslöser

Absteigende Objekte der Domäne schließen die Standardumgebung, anwenderspezifische Umgebungen, den Domänen-Koordinationsrechner und Agenten ein. Absteigende Objekte einer bestimmten Umgebung schließen anwenderspezifische Koordinationsrechner ein, Kontaktpunkte schließen Proxy-Kontaktpunkte und Hostgruppen ein.

Bestimmte, auf Domänenebene konfigurierte Einstellungen werden standardmäßig von allen oder von bestimmten absteigenden Objekten innerhalb der Domäne geerbt. Zum Beispiel können alle Umgebungen die Einstellungen der Operatorkategorien von der Domäne erben. Koordinationsrechner können Einstellungen der Operatorkategorien von ihrer Umgebung erben.

Weil Agenten über Umgebungen hinweg operieren können, kann die Vererbung direkt von der Domäne oder von der Umgebung erfolgen, je nach der Umgebungskonfiguration. Die Einstellungen der Operatorkategorie können auf Agentenebene überschrieben werden. Agenten erben die Einstellungen der Heartbeat-Signal-Häufigkeitseigenschaft direkt von der Domäne.

Normalerweise werden Konfigurationen standardmäßig vererbt. Auslöser sind eine Ausnahme. Auslöserkonfigurationen werden auf niedrigen Ebenen standardmäßig deaktiviert, können aber übernommen werden, nachdem sie aktiviert wurden.

Konfigurieren von CA EEM-Sicherheitseinstellungen für die Domäne

Die meisten CA EEM-Sicherheitseinstellungen werden während der Installation des Domänen-Koordinationsrechners eingerichtet. Eine CA EEM-Instanz verwaltet die Sicherheit für die CA Process Automation-Domäne. Deswegen gelten die gleichen Einstellungen für alle Umgebungen in der Domäne und für alle Koordinationsrechner innerhalb aller Umgebungen. Sie können die schreibgeschützten Einstellungen ändern, indem Sie den Domänen-Koordinationsrechner neu installieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.

   Die Registerkarte "Sicherheit" wird angezeigt.

2. Prüfen Sie die Einstellungen, die bei der Installation erstellt wurden. Zum Beispiel ist der Wert "EEM-Anwendungsname" der Wert, den Sie für "Anwendung" in folgenden Fällen eingeben müssen:

   - Wenn Sie sich bei CA EEM anmelden, um Anwenderkonten zu erstellen.
   - Wenn Sie neuen oder referenzierten Anwendern Standardgruppen zuweisen.

3. Überprüfen Sie den Wert für Aktualisierungsintervall der CA EEM-Cache-Aktualisierung.

   Dieser Wert drückt das Intervall zwischen Aktualisierungen des CA EEM-Zwischenspeichers in Sekunden aus. Der CA EEM-Zwischenspeicher enthält die aktuellen Anwenderkonten-, Gruppen- und Richtlinieneinstellungen aus CA Process Automation. Wenn CA EEM den Zwischenspeicher aktualisiert, werden die Inhalte des aktualisierten Zwischenspeichers an CA Process Automation gesendet. Der Standardwert, der eine optimierte Systemleistung ermöglicht, beträgt 1800 Sekunden (30 Minuten).

   - Der Standardwert ist angebracht, sobald alle Anwender in CA EEM konfiguriert sind.
   - Um diese Aufgabe schneller auszuführen, reduzieren Sie das Aktualisierungsintervall auf das Minimum (60 Sekunden), während Sie benutzerdefinierte Richtlinien testen und verfeinern. Erwägen Sie, das Intervall für die Umgebung, in der Sie testen, auf Umgebungsebene zu reduzieren.

4. Prüfen Sie den Wert "Standardmäßige Active Directory-Domäne", wenn festgelegt.

   Dieser Wert ist nur festgelegt, wenn CA EEM für die Verwendung eines externen Anwenderspeichers konfiguriert ist und wenn "Mehrfache Microsoft Active Directory-Domänen" ausgewählt ist. CA Process Automation-Anwender, die in der hier angegebenen AD-Domäne referenziert sind, können sich mit einem schlichten Anwendernamen anmelden. CA Process Automation-Anwender, die in anderen ausgewählten AD-Domänen referenziert sind, werden mit ihren Prinzipalnamen authentifiziert (d. h., *Domänenname\Anwendername*). Dieser Unterschied in den Namenskonventionen bezieht sich auch darauf, wie Anwenderidentitäten im Hauptbereich der Registerkarte "Bibliothek" referenziert sind.

5. Um eine der bearbeitbaren Werte zurückzusetzen:

   a. Wählen Sie den Knoten "Domänen" aus, und klicken Sie auf "Sperren".

   b. Wählen Sie einen neuen Wert aus.

   c. Klicken Sie auf "Speichern".

   d. Wählen Sie den Knoten "Domänen" aus, und klicken Sie auf "Entsperren".

   Wenn Sie das Aktualisierungsintervall der CA EEM-Cache-Aktualisierung reduziert haben, ziehen Sie in Erwägung, den CA Process Automation-Zwischenspeicher für Berechtigungen zu unterdrücken. Informationen finden Sie in Steuern von Zwischenspeichern von CA EEM-Aktualisierungen (siehe Seite 80).

Ändern der Sicherheitseinstellung des CA EEM-FIPS-Modus

Während der Installation wird die Eigenschaft für den CA EEM-FIPS-Modus aktiviert oder deaktiviert. Diese Einstellung bestimmt die Algorithmen, die verwendet werden, um übertragene Daten zwischen CA EEM und CA Process Automation zu verschlüsseln. Wenn FIPS-Modus aktiviert ist, sind die Algorithmen kompatibel mit FIPS 140-2. Wenn CA Process Automation mit CA EEM und einem aktivierten FIPS-Modus installiert ist, wird die Einstellung "FIPS-konformes Zertifikat" markiert angezeigt.

Sie können die Einstellung "FIPS-konformes Zertifikat" auf folgenden Ebenen ändern:

- Domäne
- Umgebungen
- Koordinationsrechner

Unabhängig von der Ebene, in der die Einstellung "FIPS-konformes Zertifikat" geändert wird, wirkt sich die Einstellung auf die gesamte Domäne aus. Die Domäne hat ein CA EEM. Die Einstellung "FIPS-konformes Zertifikat" wirkt sich auch auf die FIPS-Modus-Einstellung von CA EEM und eine iGateway-Dateieinstellung aus.

Wichtig! Wenn Sie eine CA EEM-Sicherheitseinstellung ändern, besprechen Sie dies vorher mit Ihrem Domänenadministrator. Sicherheitseinstellungen haben weitreichende Auswirkungen.

Gehen Sie folgendermaßen vor:

1. Holen Sie das EEM-Zertifikatskennwort vom Installationsprogramm ein.
2. Fahren Sie CA Process Automation auf allen Koordinationsrechnern, außer auf dem Domänen-Koordinationsrechner (sofern zutreffend), herunter.
3. Melden Sie sich bei dem Server an, auf dem der CA Process Automation-Domänen-Koordinationsrechner installiert ist, und gehen Sie folgendermaßen vor:
    a. Fahren Sie CA Process Automation herunter.
    b. Halten Sie den Koordinationsrechner-Service an. Wählen Sie beispielsweise im Windows-Startmenü "CA", "CA Process Automation 4.0" und "Koordinationsrechner-Service anhalten" aus.
4. Melden Sie sich am Server an, auf dem CA EEM installiert ist, und gehen Sie folgendermaßen vor:
    a. Fahren Sie CA EEM herunter.
    b. Halten Sie den Service "CA iTechnology iGateway" an.
5. Navigieren Sie zum Ordner "...\CA\SharedComponents\iTechnology".
6. Ändern Sie die FIPS-Modus-Einstellung in der Datei "igateway.conf".
    a. Öffnen Sie die Datei "igateway.conf", um diese zu bearbeiten. Klicken Sie zum Beispiel mit der rechten Maustaste auf "igateway.conf" und wählen Sie "Edit with Notepad++" (Mit Editor bearbeiten) aus.
    b. Suchen Sie die Zeile mit der FIPS-Modus-Einstellung. Zum Beispiel:

       ```
       Zeile 4: <FIPSMode>Deaktiviert</FIPSMode>
       ```
    c. Ändern Sie den Wert von "Deaktiviert" auf "Aktiviert" oder umgekehrt.
    d. Speichern und schließen Sie die Datei.
7. Führen Sie Hilfsprogramm "iGateway Certificate" (igwCertUtil) aus, um die CA EEM-Zertifikatstypen folgendermaßen zu konvertieren:
    - Wenn Sie den CA EEM-FIPS-Modus aktivieren (ein deaktiviertes Kontrollkästchen in ein aktiviertes Kontrollkästchen ändern), führen Sie Folgendes aus:
        - Erstellen Sie einen "pem"-Zertifikatstyp, "PAM.cer" und "PAM.key".
        - Ersetzen Sie das Zertifikat "PAM.p12" mit dem "pem"-Zertifikatstyp.
    - Wenn Sie den CA EEM-FIPS-Modus deaktivieren (ein aktiviertes Kontrollkästchen in ein deaktiviertes Kontrollkästchen ändern), ersetzen Sie "PAM.cer" und "PAM.key" durch "PAM.p12" und ein Kennwort.

      Hinweis: Details finden Sie in Beispiele für die Verwendung des iGateway Certificate-Hilfsprogramms (siehe Seite 154).

8. Starten Sie den iGateway-Service neu.
9. Starten Sie CA EEM mit der entsprechenden FIPS-Modus-Einstellung neu.
10. Starten Sie den Koordinationsrechner-Service auf dem Server mit dem Domänen-Koordinationsrechner neu.
    - Stoppen Sie den Koordinationsrechner (siehe Seite 206).
    - Starten Sie den Koordinationsrechner (siehe Seite 207).
11. Melden Sie sich bei CA Process Automation an, und zeigen Sie die Sicherheitseinstellung für das FIPS-konforme Zertifikat und zugehörige Einstellungen folgendermaßen an:
    a. Melden Sie sich bei CA Process Automation an, und klicken Sie auf die Registerkarte "Konfiguration".
    b. Navigieren Sie zu der Ebene, auf der Sie die Änderung implementieren und diese Ebene sperren möchten (Domäne, Umgebung oder Koordinationsrechner).
    c. Zeigen Sie das Kontrollkästchen "FIPS-konformes Zertifikat" an.
    d. Wenn es sich bei Ihrer Änderung um das Aktivieren des FIPS-Modus für CA EEM handelt, führen Sie Folgendes aus:
       - Stellen Sie sicher, dass ""FIPS-konformes Zertifikat"" ausgewählt ist. Wenn dies nicht der Fall ist, aktivieren Sie es.
       - Geben Sie den generierten Schlüssel in das Feld "CA EEM-Zertifikatsschlüssel" ein.
    e. Wenn es sich bei Ihrer Änderung um das Deaktivieren des FIPS-Modus für CA EEM handelt, führen Sie Folgendes aus:
       - Stellen Sie sicher, dass ""FIPS-konformes Zertifikat"" deaktiviert ist. Wenn dies nicht der Fall ist, deaktivieren Sie es.
       - Geben Sie das generierte Kennwort in das Feld "CA EEM-Zertifikatskennwort" ein.
    f. Klicken Sie auf "Speichern".
    g. Entsperren Sie die Ebene, das heißt "Domäne", "Umgebung" vom Auswahlmenü "Browser" oder "Koordinationsrechner" vom Auswahlmenü "Koordinationsrechner".
12. Starten Sie CA Process Automation auf Servern mit Koordinationsrechnern, die nicht der Domänen-Koordinationsrechner sind, neu.

Beispiele für die Verwendung des iGateway Certificate-Hilfsprogramms

Sie können die Sicherheitseinstellung des CA EEM-FIPS-Modus von der Einstellung ändern, die bei der Installation konfiguriert wurde. Teil dieses Änderungsprozesses ist das Verwenden des Hilfsprogramms "iGateway Certificate" (igwCertUtil). Diese Datei befindet sich unter "...\CA\SharedComponents\iTechnology\igwCertUtil.exe".

Hinweis: Weitere Informationen finden Sie unter Ändern der Sicherheitseinstellung des CA EEM-FIPS-Modus (siehe Seite 151).

Das Hilfsprogramm "iGateway Certificate" enthält Funktionen, die in folgenden Beispielen beschrieben werden:

Beispiel: Erstellen Sie einen pem-Zertifikatstyp mit den Dateien "PAM.cer" und "PAM.key".

Das folgende "igwCertUtil"-Beispiel erstellt ein pem-Zertifikat mit einer ".cer"-Datei und einer ".key"-Datei.

```
igwCertUtil -version 4.6.0.0
-create -cert
    "<Certificate>
        <certType>pem</certType>
        <certURI>PAM.cer</certURI>
        <keyURI>PAM.key</keyURI>
        <subject>CN=PAM</subject>
    </Certificate>"
```

Beispiel: Erstellen Sie einen pem-Zertifikatstyp für einen Aussteller

Das folgende igwCertUtil-Beispiel erstellt ein Zertifikat, in dem der genannte Aussteller in der Datei "issuer.cer" und in der Datei "issuer.key" angegeben ist.

```
igwCertUtil -version 4.6.0.0
-create -cert
    "<Certificate>
        <certType>pem</certType>
        <certURI>PAM.cer</certURI>
        <keyURI>PAM.key</keyURI>
        <subject>CN=PAM</subject>
    </Certificate>"
-issuer
    "<Certificate>
        <certType>pem</certType>
        <certURI>issuer.cer</certURI>
        <keyURI>issuer.key</keyURI>
    </Certificate>"
```

Beispiel: Kopieren Sie "PAM.cer" mit "PAM.key" nach "PAM.p12"

Im folgenden Beispiel kopiert das Hilfsprogramm "igwCertUtil" das pem-Zertifikat zum Zielzertifikat "p12". Das pem-Zertifikat schließt den Namen der Datei ".cer" und der Datei ".key" ein. Das p12-Zertifikat schließt die Namens- und Kennwortkombination ein.

```
igwCertUtil -version 4.6.0.0
-copy -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

Beispiel: Konvertieren Sie "PAM.cer" und "PAM.key" in "PAM.p12" und ein Kennwort

Im folgenden Beispiel konvertiert das Hilfsprogramm "igwCertUtil" den pem-Zertifikatstyp in einen p12-Zertifikatstyp. Das Hilfsprogramm konvertiert "PAM.cer" in "PAM.p12" und konvertiert "PAM.key" in ein Kennwort.

```
igwCertUtil -version 4.6.0.0
-conv -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

Konfigurieren von Domäneneigenschaften

Die Domäne ist das Stammelement in der CA Process Automation-Hierarchie. Sie können gewisse Domäneneigenschaften bearbeiten, beispielsweise die Häufigkeit, mit der Agenten den Domänen-Koordinationsrechner darüber benachrichtigen, dass sie aktiv sind. Wenn beispielsweise der Wert für das Heartbeat-Signal von 2 in 3 geändert wird, kann der Netzwerkverkehr reduziert werden. Die Einstellung, die Sie auf Domänenebene angeben, kann auf Umgebungsebene geerbt oder überschrieben werden.

Hinweis: Informationen zu Feldbeschreibungen finden Sie im *Benutzeroberflächen-Referenzhandbuch*.

Die Inhaltsadministratoren in der Gruppe "PAMAdmins" können die Domäne sperren und Domäneneigenschaften bearbeiten. Die Domain_Admin-Berechtigung in der CA EEM-Domänenrichtlinie gewährt Autorisierung.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.

   Das Auswahlmenü Konfigurationsbrowser wird geöffnet, und der Knoten Domäne ist ausgewählt.

2. Klicken Sie auf die Registerkarte Eigenschaften.

3. Zeigen Sie die schreibgeschützten Felder an, zum Beispiel:

   a. Prüfen Sie die Eingabe für Domänen-URL. Diese Eingabe ist der erste Teil der URL, die Sie verwenden, um zu CA Process Automation zu navigieren. Die Eingabe für Domänen-URL kann entweder den Domänen-Koordinationsrechner oder den Lastenausgleich identifizieren. Die URL kann sicher oder normal sein.

   b. Prüfen Sie die Eingabe für Hostname. Diese Eingabe gibt den Host an, auf dem der Domänen-Koordinationsrechner installiert ist.

   c. Prüfen Sie die Eingabe für Koordinationsrechner-Name. Auf Domänenebene ist diese Eingabe standardmäßig der Domänen-Koordinationsrechner.

   d. Prüfen Sie die Eingabe für Status. Der Domänenstatus kann Werte wie "Aktiv" oder "Gesperrt durch *Anwender-ID*" haben.

4. Klicken Sie bei ausgewähltem Knoten Domäne auf Sperren.

   Wenn Sie die Domäne sperren, können nur Sie die Domäneneigenschaften bearbeiten.

5. Um die Einstellung Heartbeat-Intervall (Minuten) zu bearbeiten, wählen Sie einen neuen Wert aus dem Spinner-Feld aus.

   Wenn Sie einen neuen Wert festlegen, wird geändert, wie oft Agenten ein Heartbeat-Signal an den Domänen-Koordinationsrechner senden. Standardmäßig senden Agenten alle 2 Minuten ein Heartbeat-Signal. Diese Konfiguration bezieht sich auf alle Agenten in der Domäne, doch Sie können diesen Wert für einzelne Agenten überschreiben. Wenn Sie den Wert erhöhen, reduziert sich der Netzwerkverkehr. Wenn Sie das Intervall auf ein Mal pro Minute erhöhen, können Sie Agentenprobleme schneller identifizieren.

6. Ziehen Sie in Erwägung, die standardmäßige Einstellung für Kontaktpunktsicherheit (Deaktiviert) auf Domänenebene beizubehalten.

   Das Einstellung "Aktiviert" gibt an, dass Anwenderrechte für Ziele in einem bestimmten Prozess verifiziert und durchgesetzt werden müssen. Die Anwenderrechte werden in einer anwenderspezifischen CA EEM-Richtlinie konfiguriert, die die Ressourcenklasse "Kontaktpunktsicherheit" verwendet. Sie können Ausführungsrechte für Anwender oder Gruppen für eine spezifische Umgebung oder einen spezifischen Kontaktpunkt gewähren.

   Hinweis: Informationen finden Sie im Thema zur Vorgehensweise zum Konfigurieren der Kontaktpunktsicherheit (siehe Seite 160).

7. Konfigurieren Sie die Hostgruppen-Ziele unter Berücksichtigung der folgenden Richtlinien:

   ■ Deaktivieren Sie die Eigenschaft Ziel nur in Hostgruppen abgleichen?, wenn das Muster, das für Hostgruppen konfiguriert ist, manchmal mit den IP-Adressen oder Hostnamen von folgenden Arten von Hosts übereinstimmt:

     – Hosts, die Agenten installiert haben, die zu Kontaktpunkten zugeordnet sind.

     – Remote-Hosts, die mit Agenten verbunden sind, die zu Proxy-Kontaktpunkten zugeordnet sind.

     Hinweis: In diesem Fall deaktiviert das Produkt Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen? standardmäßig.

   ■ Aktivieren Sie die Eigenschaft Ziel nur in Hostgruppen abgleichen?, wenn das Muster, das für Hostgruppen konfiguriert ist, selten mit den IP-Adressen oder Hostnamen von folgenden Arten von Hosts übereinstimmt:

     – Hosts, die Agenten installiert haben, die zu Kontaktpunkten zugeordnet sind.

     – Remote-Hosts, die mit Agenten verbunden sind, die zu Proxy-Kontaktpunkten zugeordnet sind.

   ■ Deaktivieren Sie die Eigenschaft Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen?, wenn Inhaltsdesigner normalerweise die folgenden Konventionen verwenden:

     – Sie verwenden einen Hostnamen, wenn der Mustertyp, der in der Hostgruppen-Konfiguration verwendet wird, ein Namensmuster für Hosts ist.

     – Sie verwenden eine IP-Adresse, wenn der Mustertyp, der in der Hostgruppen-Konfiguration verwendet wird, ein Teilnetz, ein IP-Adress-Bereich oder eine Liste von IP-Adressen ist.

   ■ Aktivieren Sie die Eigenschaft Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen?, wenn sich Inhaltsdesigner dessen bewusst sind, dass Hostgruppen auf spezifische Hosts verweisen, jedoch nicht unbedingt wissen, auf welche Art. Das Aktivieren der Eigenschaft stellt sicher, dass der Operator einen Zielhost finden kann. Zum Beispiel kann ein Operator, der den Host als IP-Adresse angibt, das Ziel finden, wenn die Hostgruppe mit einem Namensmuster für Hosts verweist.

8. Geben Sie Anforderungen für die Bereinigung von Berichtsdaten an, die in dieser Domäne generiert wurden. Alternativ können Sie Berichtsdaten nach Bedarf reinigen, indem Sie den Datumsbereich angeben, in dem die Berichte generiert wurden.

   a. Geben Sie im Feld Option zum Bereinigen von Berichtsdaten an, ob Berichtsdaten täglich bereinigt werden sollen. Wenn Sie Berichtsdaten täglich bereinigen auswählen, geben Sie die Uhrzeit an, zu der die Bereinigung starten soll. Um die Bereinigung beispielsweise um 18:30 zu starten, geben Sie im Feld Startzeit für das tägliche Bereinigen von Berichtsdaten "18:30" (im 24-Sunden-Format) an.

   b. Wenn Sie einen Bereinigungsablaufplan angegeben haben, geben Sie die Anzahl der Tage an, die die Berichtsdaten beibehalten werden sollen, bevor die Bereinigung durchgeführt wird. Zum Beispiel legt eine Eingabe von "14" im Feld Anzahl der Tage zum Beibehalten von Berichtsdaten fest, dass alle Berichtsdaten bereinigt werden sollen, die älter als zwei Wochen sind.

   c. Klicken Sie auf die Schaltfläche Berichtsdaten löschen, geben Sie einen Datumsbereich für die Berichtsdaten an, die gelöscht werden sollen, und klicken Sie auf OK.

9. Um die Berichterstellung für Prozesse zu generieren, aktivieren Sie das Kontrollkästchen "Prozess-Berichterstattung aktivieren". Um diese Funktion zu deaktivieren, deaktivieren Sie das Kontrollkästchen Prozess-Berichterstattung aktivieren.

10. Um Berichterstellungsdaten für Operatoren zu generieren, aktivieren Sie das Kontrollkästchen "Operator-Berichterstattung aktivieren". Um diese Funktion zu deaktivieren, deaktivieren Sie das Kontrollkästchen Operator-Berichterstattung aktivieren.

11. Um zu erlauben, dass das Produkt Inhaltsdesignern in der Designumgebung Prozessprotokolle anzeigt, aktivieren Sie das Kontrollkästchen Prozessprotokolle aktivieren. Um Protokolle zu Laufzeit-Prozessinstanzen für die Produktionsumgebung auf Umgebungsebene zu verbergen, deaktivieren Sie das Kontrollkästchen Prozessprotokolle aktivieren.

12. Um die Operator-Wiederherstellung zu automatisieren, akzeptieren Sie den Standard für die Eigenschaft Operator-Wiederherstellung Aktivieren.

13. Klicken Sie auf "Speichern".

14. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Ansatz beim Konfigurieren der Kontaktpunktsicherheit

Kontaktpunktsicherheit ist eine Eigenschaft der Domänenebene. Standardmäßig wird Kontaktpunktsicherheit nicht durchgesetzt. Dies ermöglicht es vorhandenen Prozessen, erfolgreich ausgeführt zu werden.

Hinweis: Wenn Sie das Durchsetzen der Kontaktpunktsicherheit festlegen und keine Richtlinien zur Kontaktpunktsicherheit in CA EEM vorhanden sind, liegt kein Schutz vor.

Normalerweise sind geschäftskritische Hosts und Hosts mit streng vertraulichen Daten nur in einer Produktionsumgebung vorhanden. Wenn Sie Ihre CA Process Automation-Domäne in eine Designumgebung und eine Produktionsumgebung partitioniert haben, berücksichtigen Sie diese Richtlinien:

- Designumgebung: Akzeptieren Sie die vererbten Einstellungen, bei denen Kontaktpunktsicherheit deaktiviert ist
- Produktionsumgebung: Aktivieren Sie Kontaktpunktsicherheit in den Umgebungseigenschaften. Erstellen Sie dann eine globale Richtlinie zur Kontaktpunktsicherheit, die angegebene Gruppen oder Anwender zur Ausführung von Operatoren in ausgewählten Kategorien autorisiert. Geben Sie die Umgebung als Filter an. Geben Sie anschließend einen Filter für jeden Kontaktpunkt an, der einem unternehmenskritischen Host zugeordnet ist.

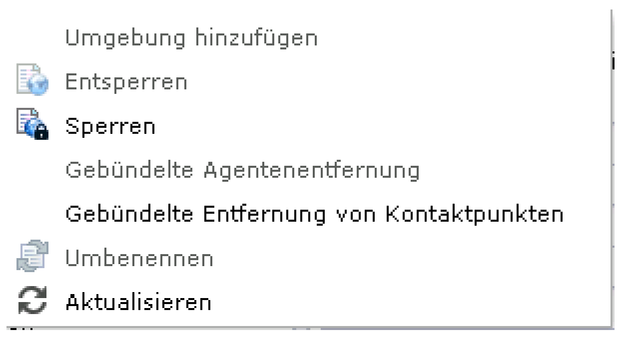
Alternativ können Sie "Kontaktpunktsicherheit" in einer Entwicklungs- oder Testumgebung verwenden, um festzulegen, wer Prozesse auf Ihrem Koordinationsrechner ausführen kann. In diesem Fall könnten Sie eine Richtlinie erstellen und alle Mitglieder Ihrer Teams als Identitäten auflisten. In dieser Richtlinie erstellen Sie zwei Filter. Sie erstellen einen für Ihren Koordinationsrechner als Kontaktpunkt und einen anderen für Ihre Umgebung.

Verwalten der Domänenhierarchie

Standardmäßig verfügen alle Administratoren, die der PAMAdmins-Gruppe zugewiesen sind, über die Berechtigungen "Domain_Admin". Wenn Sie anwenderdefinierte Richtlinien und Gruppen verwenden, können Sie die Berechtigungen "Domain_Admin" auf ausgewählte Administratoren beschränken.

Aufgaben, die nur ein Anwender mit den Berechtigungen "Domain_Admin" ausführen kann, sind Aktionen, bei denen das Sperren der Domäne erforderlich ist. Weitere Informationen finden Sie unter Sperren und Entsperren der Domäne (siehe Seite 147).

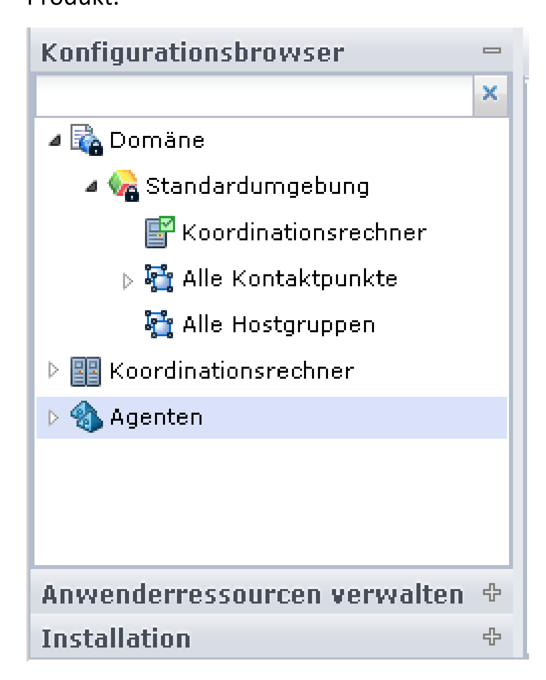
Diese Aufgaben ändern die Domänenhierarchie, indem ein Knoten umbenannt, hinzugefügt oder entfernt wird.



- Umgebung hinzufügen: Weitere Informationen finden Sie unter Hinzufügen einer Umgebung zur Domäne (siehe Seite 164).
- Umgebung entfernen: Weitere Informationen finden Sie unter Entfernen einer Umgebung aus der Domäne (siehe Seite 165).
- Gebündelte Agentenentfernung: Weitere Informationen finden Sie unter Gebündeltes Entfernen ausgewählter Agenten (siehe Seite 228).
- Gebündelte Entfernung von Kontaktpunkten: Weitere Informationen finden Sie unter Gebündeltes Entfernen nicht verwendeter leerer Kontaktpunkte (siehe Seite 248).
- Domäne umbenennen: Weitere Informationen finden Sie unter Umbenennen von Domänen (siehe Seite 166).

Informationen über Domänenhierarchie, Koordinationsrechner und Agenten

Das Auswahlmenü "Konfigurationsbrowser" auf der Registerkarte "Konfiguration" enthält ein Stammobjekt, das während der Installation den Namen "Domäne" erhält. Die Domäne ist das übergeordnete Element für alle konfigurierbaren Elemente im Produkt.



Der Konfigurationsbrowser zeigt physische und logische Entitäten an.

Physisch

Eine *physische* Komponente ist eine installierte Komponente (ein Koordinationsrechner oder ein Agent).

Koordinationsrechner

Domänen-Koordinationsrechner

Direkt nach der Installation ist der Domänen-Koordinationsrechner die einzige physische Komponente.

Andere Koordinationsrechner

Administratoren können andere Koordinationsrechner über das Auswahlmenü "Installation" installieren.

Agenten

Administratoren können Agenten über das Auswahlmenü "Installation" installieren.

Logischer Operator

Eine oder mehrere *logische* Entitäten bilden die Domänenhierarchie, die aus mindestens einer Umgebung besteht. Jede Umgebung hat einen oder mehrere Koordinationsrechner-Kontaktpunkte und kann Kontaktpunkte und Hostgruppen haben, die zu Agenten zugeordnet sind.

Domäne

Die Domäne ist der Stammknoten der Domänen-Hierarchie. Das Produkt hat eine Domäne.

Standardumgebung

Die Standardumgebung ist die Umgebung, die das Installationsprogramm erstellt.

Koordinationsrechner (Kontaktpunkt)

Während der Installation zeigt das Produkt unter "Standardumgebung" den Koordinationsrechner-Kontaktpunkt an, der den Domänen-Koordinationsrechner mit der Standardumgebung zuordnet. Jeder Koordinationsrechner benötigt einen separaten Kontaktpunkt.

Hinweis: Das Produkt ordnet die Umgebung für einen geclusterten Koordinationsrechner-Kontaktpunkt zum Kontaktpunkt für diesen Cluster zu. Wenn Sie einen solchen Kontaktpunkt als Operatorziel verwenden, wählt der Lastenausgleich den Zielknoten aus.

Alle Kontaktpunkte

Während der Installation ist der Knoten "Alle Kontaktpunkte" leer. Von einem installierten Agenten können Sie einen Kontaktpunkt in einer ausgewählten Umgebung konfigurieren. Kontaktpunkte verbinden Agenten mit Umgebungen. Der Knoten "Alle Kontaktpunkte" unter "Standardumgebung" enthält nur Kontaktpunkte, die der "Standardumgebung" zugeordnet sind. Einem Agenten können mehrere Kontaktpunkte zugeordnet sein. Mehreren Agenten kann ein einzelner Kontaktpunkt zugeordnet sein.

Alle Hostgruppen

Während der Installation ist der Knoten "Alle Hostgruppen" leer. Von einem installierten Agenten können Sie eine Hostgruppe in einer ausgewählten Umgebung erstellen, und Sie können die Eigenschaften der Hostgruppen konfigurieren. Für die Konnektivität von einem Agenten zu einer Gruppe von Remote-Hosts ist ein Anwenderkonto auf jedem Remote-Host erforderlich. Die Anwenderkonten werden mit den Anmeldeinformationen konfiguriert, die in den Eigenschaften der Hostgruppen angegeben sind.

Andere Umgebung

Sie können eine separate Produktionsumgebung hinzufügen. Jede Umgebung erfordert mindestens einen Koordinationsrechner-Kontaktpunkt.

Andere Elemente "Koordinationsrechner (Kontaktpunkte)", andere Elemente "Alle Kontaktpunkte", andere Elemente "Alle Hostgruppen" in der neuen Umgebung

Für jeden installierten Koordinationsrechner erstellen Sie einen Kontaktpunkt unter einer ausgewählten Umgebung. Die Koordinationsrechner-Kontaktpunkte werden unter dem Knoten der von Ihnen ausgewählten Umgebung angezeigt. Alle von Ihnen erstellten Agentenkontaktpunkte werden unter "Alle Kontaktpunkte" für diese Umgebung angezeigt. Alle von Ihnen erstellten Hostgruppen werden unter "Alle Hostgruppen" für diese Umgebung angezeigt.

Inhaltsadministratoren automatisieren Prozesse, indem sie Operatoren erstellen und verknüpfen. Operatoren verwenden normalerweise einen angegebenen Koordinationsrechner-Kontaktpunkt (bzw. sie werden darauf ausgeführt) als Ziel. Ein Operator kann auf einen Kontaktpunkt als Ziel verwenden, der mit mehreren Agenten verbunden ist. In diesem Fall kann dieser Operator potenziell auf einem zugeordneten Agentenhost ausgeführt werden.

Hinzufügen einer Umgebung zur Domäne

Administratoren können der Domäne eine Umgebung hinzufügen. Normalerweise fügen Administratoren eine Produktionsumgebung hinzu.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".

   Das Auswahlmenü zeigt das Domänensymbol mit einem Vorhängeschloss an, um anzugeben, dass die Domäne gesperrt ist.

2. Klicken Sie mit der rechten Maustaste auf die Domäne, und klicken Sie auf Umgebung hinzufügen.

3. Geben Sie im Dialogfeld Neue Umgebung hinzufügen einen Namen für die neue Umgebung ein, und klicken Sie auf OK.

   Im Auswahlmenü Konfigurationsbrowser wird der Name der neuen Umgebung mit Knoten zum Hinzufügen von "Alle Kontaktpunkte" und "Alle Hostgruppen" angezeigt. Am Anfang hat die neue Umgebung keinen Koordinationsrechner.

4. Klicken Sie auf "Speichern".

5. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Entfernen einer Umgebung aus der Domäne

Mit Domänenadministratorrechten können Sie eine Umgebung aus der Domäne löschen. Wenn die Umgebung aktiv verwendet wird, nehmen Sie die erforderlichen Schritte vor, um Bibliotheksobjekte und Ausführungsziele zu beizubehalten.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie mit der rechten Maustaste auf die Domäne, und klicken Sie auf Sperren.
3. Überprüfen Sie die Operatoren in aktiven Prozessen, die auf einen Koordinationsrechner oder auf einen Kontaktpunkt in der Zielumgebung zielen.
4. Sie müssen die Kontaktpunkte, Proxy-Kontaktpunkte, Hostgruppen und Kontaktpunktgruppen, die zur Zielumgebung zugeordnet sind, neu konfigurieren oder entfernen. Ordnen Sie zum Beispiel Agentenkontaktpunkte zu einer anderen Umgebung zu.
5. Verschieben Sie den Bibliotheksinhalt nach Bedarf in eine andere Umgebung.

   Hinweis: Die folgenden Themen beschreiben, wie sie Inhalte verschieben:

   - Exportieren von Ordnern (siehe Seite 379)
   - Importieren von Ordnern (siehe Seite 381)
6. Entfernen Sie jeden Koordinationsrechner aus der Umgebung:

   a. Stellen Sie den Koordinationsrechner unter Quarantäne (siehe Seite 204).

   b. Entfernen Sie den Koordinationsrechner aus einer Umgebung (siehe Seite 179).
7. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie Löschen aus.
8. Klicken Sie in der Bestätigungsmeldung auf Ja.
9. Klicken Sie auf "Speichern".
10. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Umbenennen von Domänen

In der Dokumentation und Hilfe verwenden wir den Namen "Domäne", um auf die CA Process Automation-Domäne zu verweisen. Administratoren mit den Berechtigungen "Domain_Admin" können diesen oberen Knoten der Domänenhierarchie umbenennen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
3. Klicken Sie mit der rechten Maustaste auf "Domäne", und wählen Sie "Umbenennen" aus.
4. Geben Sie den neuen Namen in das Feld ein, das die Domäne enthält.
5. Klicken Sie auf "Speichern".
6. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Kapitel 6: Verwalten von Umgebungen

Bei der Installation verfügt die CA Process Automation-Domäne über eine Umgebung, die Standardumgebung. Administratoren, die in der standardmäßigen PAMAdmins-Gruppe definiert sind, haben alle Rechte. Sie können CA EEM-Richtlinien erstellen, die verschiedenen Anwendern bestimmte Administratorrechte gewähren. Beispiel:

- Ein Administrator mit *Domänenadministratorrechten* kann zusätzliche Umgebungen erstellen, um die Domäne aufzuteilen. Normalerweise wird die Standardumgebung verwendet, um automatische Prozesse zu entwerfen und Objekte zu unterstützen. Wenn ein oder mehrere Prozesse zur Verwendung in der vorhandenen Produktionsumgebung bereit sind, erstellt der Administrator eine Umgebung in CA Process Automation und benennt sie "Produktionsumgebung". Andere Beispiele hierfür sind eine geografische Segmentierung, eine Segmentierung nach Lebenszyklus und Staging. Diese Aufgaben werden in diesem Kapitel beschrieben.
- Ein Administrator mit den Rechten eines *Umgebungsinhalts-Administrators* kann Kontaktpunkte und Hostgruppen hinzufügen, Kontaktpunktgruppen erstellen sowie nicht verwendete Kontaktpunkte gebündelt entfernen. Er kann zudem neue Objekte wie Prozesse und Ablaufpläne erstellen. In den nachfolgenden Kapiteln finden Sie Informationen zu Kontaktpunkten und Hostgruppen. Im *Handbuch für Inhaltsdesign* finden Sie weitere Informationen über die Registerkarten "Bibliothek" und "Designer" für das Erstellen und Entwickeln von Inhalten.
- Ein Administrator mit den Rechten eines *Umgebungskonfigurations-Administrators* kann die Inhalte einer ausgewählten Umgebung konfigurieren. Administratoren können übernommene Einstellungen akzeptieren oder überschreiben. Das Konfigurieren von Inhalten einer Umgebung kann das Bearbeiten der Sicherheitseinstellungen, das Festlegen der Umgebungseigenschaften, das Aktivieren oder Deaktivieren von Operatorkategorien und das Festlegen der Vererbung für Auslöser enthalten.

Dieses Kapitel enthält folgende Themen:

Konfigurieren der Inhalte einer Umgebung

Wenn Sie eine Umgebung im Konfigurationsbrowser auswählen, werden folgende Registerkarten unter "Inhalte" von "<Umgebungsname>" angezeigt:

Inhalt von "Standardumgebung"

Sicherheit | Automatisches ... | Eigenschaften | Module | Auslöser | Audit-Pfade

- Sicherheit

  Weitere Informationen finden Sie unter Anzeigen oder Zurücksetzen der Sicherheitseinstellungen für eine ausgewählte Umgebung (siehe Seite 168).

- Automatisches Zulassen

  Weitere Informationen finden Sie unter Gebündeltes Hinzufügen von Kontaktpunkten für Agenten (siehe Seite 245).

- Eigenschaften

  Weitere Informationen finden Sie unter Konfigurieren von Umgebungseigenschaften (siehe Seite 169).

- Module

  Weitere Informationen finden Sie unter Aktivieren einer Operatorkategorie und Überschreiben von übernommenen Einstellungen (siehe Seite 173).

- Auslöser

  Weitere Informationen finden Sie unter Angeben von Auslösereinstellungen für Umgebungen (siehe Seite 174).

- Audit-Pfade

  Weitere Informationen finden Sie unter Anzeigen des Audit-Pfads für eine Umgebung (siehe Seite 360).

Anzeigen oder Zurücksetzen der Sicherheitseinstellungen für eine ausgewählte Umgebung

Die meisten Einstellungen der Registerkarte "Sicherheit" werden während der Installation oder des Upgrades des Domänen-Koordinationsrechners erstellt. Sie können diese schreibgeschützten Einstellungen nur ändern, indem Sie den Domänen-Koordinationsrechner neu installieren.

Jede Umgebung übernimmt die Einstellungen, die Sie während der Installation des Domänen-Koordinationsrechners vorgenommen haben. Wenn Sie das Kontrollkästchen "Erben" deaktivieren, können Sie das Aktualisierungsintervall der CA EEM-Cache-Aktualisierung (in Sekunden) aktualisieren. Wenn Sie das Aktualisierungsintervall verkürzen, spiegelt CA Process Automation Änderungen, die Sie in CA EEM vornehmen, schneller wider.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie im Auswahlmenü "Konfigurationsbrowser" die Option "Domäne" ein, und wählen Sie dann die Zielumgebung aus.

   Die Registerkarte "Sicherheit" wird geöffnet.

3. Prüfen Sie die Sicherheitseinstellungen, die während des Installationsprozesses vorgenommen wurden.

4. (Optional) Aktualisieren Sie den Wert für Aktualisierungsintervall der CA EEM-Cache-Aktualisierung.

   a. Klicken Sie auf Sperren.

   b. Deaktivieren Sie das Kontrollkästchen Erben.

   c. Aktualisieren Sie den Wert.

   d. Klicken Sie auf "Speichern".

   e. Wählen Sie die Umgebung aus, und klicken Sie auf "Entsperren".

   Hinweis: Wenn Sie das Aktualisierungsintervall der CA EEM-Cache-Aktualisierung reduziert haben, ziehen Sie in Erwägung, den CA Process Automation-Zwischenspeicher für Berechtigungen zu unterdrücken. Informationen finden Sie in Steuern von Zwischenspeichern von CA EEM-Aktualisierungen (siehe Seite 80).

Konfigurieren von Umgebungseigenschaften

Konfigurieren der Eigenschaften für eine ausgewählte Umgebung über die Registerkarte "Konfiguration". Die Rechte eines Umgebungskonfigurations-Administrators sind erforderlich, um Umgebungseigenschaften zu konfigurieren oder um die Einstellungen auf einer Ebene, die von der Umgebung erben kann, zu überschreiben.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.

2. Erweitern Sie den Knoten "Domäne", klicken Sie mit der rechten Maustaste auf den entsprechenden Umgebungsnamen, und klicken Sie auf "Sperren".

3. Klicken Sie auf die Registerkarte "Eigenschaften", und zeigen Sie dann die Eigenschaften an oder aktualisieren Sie sie nach Bedarf.

   Automatische Operator-Wiederherstellung

   Gibt an, ob die Wiederherstellung automatisiert werden soll. Die Wiederherstellung gilt für spezifische Operatoren, die mit einem SYSTEM_ERROR fehlschlagen und wiederherstellbare Prozesse im Zustand "Blockiert", "Wird ausgeführt" oder "Im Wartezustand" haben. Wählen Sie "Wahr" aus, um die Wiederherstellung zu starten, wenn der inaktive Koordinationsrechner oder Agent aktiv wird. Bei der Wiederherstellung werden Operatoren zurückgesetzt, die den Zustand SYSTEM_ERROR aufweisen, und ihre Prozesse werden fortgesetzt. Die zurückgesetzten Operatoren in einem fortgesetzten Prozess beginnen, auf den zugeordneten Zielen ausgeführt zu werden. Die Operatorziele können Koordinationsrechner, Kontaktpunkte, Hosts sein, die mit Proxy-Kontaktpunkten oder Hosts in einer Hostgruppe verbunden sind.

   Werte: Diese Eigenschaft hat folgende Werte:

   - **Aktiviert**: Die Wiederherstellung wird automatisiert.
   - **Deaktiviert**: Die automatische Wiederherstellung wird verhindert.

   Standard: Aktiviert.

   Kontaktpunktsicherheit

   Gibt an, ob der Wert, der in den Domäneneigenschaften konfiguriert ist, vererbt werden soll oder ob der Wert auf der Umgebungsebene auf "Wahr" oder "Falsch" festgelegt werden soll.

   Werte: Diese Eigenschaft hat folgende Werte:

   - **Von Domäne erben**: Verwenden Sie den Wert, der für dieses Feld in den Domäneneigenschaften konfiguriert ist.
   - **Aktiviert**: Die Richtlinien für Kontaktpunktsicherheit für dieses Ziel werden durchgesetzt, und der Zugriff wird nur gewährt, wenn dem Anwender diese Berechtigung erteilt wurde.
   - **Deaktiviert**: Nicht überprüfen, ob der Anwender, der den Prozess ausführt, über Ausführungsrechte für das aktuelle Ziel verfügt.

   Standard: Von Domäne übernehmen.

Ziel nur in Hostgruppen abgleichen?

Gibt den Suchbereich für ein Operatorziel an, wenn die Eingabe im Feld "Ziel" eine IP-Adresse oder ein Hostname (FQDN) ist. Die Ausführung des Operators auf dem Ziel kann nur fortfahren, wenn das Ziel CA Process Automation bekannt ist. Wählen Sie "Deaktiviert" aus, um eine möglichst umfassende Suche zu ermöglichen. Wählen Sie hier "Aktiviert" und für das nächste Feld "Deaktiviert" aus, um die Suche möglichst eingeschränkt zu gestalten.

Hinweis: Eine DNS-Suche mit einem angegebenen Hostnamen findet zugeordnete IP-Adressen; eine DNS-Suche mit der IP-Adresse findet zugeordnete Hostnamen.

Werte: Diese Eigenschaft hat folgende Werte:

- **Von Domäne erben**: Verwenden Sie den Wert, der für dieses Feld in den Domäneneigenschaften konfiguriert ist.
- **Aktiviert**: Der Bereich der Suche hängt davon ab, ob das Feld "Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen" aktiviert oder deaktiviert ist.

  Wenn eine DNS-Suche deaktiviert ist - Suche: Hostgruppe verweist auf einen Remote-Host (exakte Übereinstimmung)

  Wenn eine DNS-Suche aktiviert ist - Suche: Hostgruppe verweist auf einen Remote-Host (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)
- **Deaktiviert**: Die Domänenkomponenten werden in der folgenden Reihenfolge durchsucht:

  Kontaktpunkt (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Koordinationsrechner (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Agent (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Ein Proxy-Kontaktpunkt, der zu einem Remote-Host zugeordnet ist (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Hostgruppenreferenz auf einen Remote-Host (exakte Übereinstimmung oder Ergebnis der DNS-Suche)

Standard: Von Domäne übernehmen.

Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen?

Hinweis: Dieses Feld wird aktiviert, wenn "Ziel nur in Hostgruppen abgleichen" auf "Aktiviert" gesetzt ist.

Gibt an, ob das Durchsuchen von Hostgruppenreferenzen auf einen Eingabetyp beschränkt werden soll. Zum Beispiel: Wenn der Feld Eingabetyp im Feld "Ziel" ein FQDN ist, wird nur nach Namensmustern für Hosts gesucht. Wenn der Feld Eingabetyp im Feld "Ziel" eine IP-Adresse ist, wird nur nach Teilnetzen gesucht. Wenn eine DNS-Suche eingeschlossen ist, kann die Suche gemäß der Auflösung durch die DNS-Suche auch Hostgruppenreferenzen auf den anderen Typ akzeptieren.

Werte: Diese Eigenschaft hat folgende Werte:

- **Von Domäne erben**: Verwenden Sie den Wert, der für dieses Feld in den Domäneneigenschaften konfiguriert ist.
- **Aktiviert**: Alle Hostgruppenreferenzen werden durchsucht. Hostgruppenreferenzen für Hostnamen sind Muster (reguläre Ausdrücke), die den angegebenen Hostnamen enthalten können. Hostgruppenreferenzen für IP-Adressen sind IP-Adressteilnetze, die in CIDR-Notationen ausgedrückt werden, die die angegebene IP-Adresse enthalten können. Dehnen Sie die Suche auf alle Hostgruppenreferenzen aus. Legen Sie fest, ob die Suche eine genaue Übereinstimmung oder eine Übereinstimmung mit dem Ergebnis der DNS-Suche finden soll.
- **Deaktiviert:** Schränkt die Suche auf Hostgruppenreferenzen ein, die eine genaue Übereinstimmung mit der Eingabe im Feld "Ziel" enthalten.

Standard: Von Domäne übernehmen.

4. Klicken Sie auf "Speichern".
5. Wählen Sie die Umgebung aus, und klicken Sie auf "Entsperren".

   Die Aktualisierungen der Umgebungseigenschaft sind aktiv.

Aktivieren einer Operatorkategorie und Überschreiben von übernommenen Einstellungen

Die Einstellungen der Operatorkategorien werden in einer Umgebung standardmäßig als "Von Domäne erben" angezeigt. Wenn Einstellungen der Operatorkategorien auf Domänenebene konfiguriert werden, kann ein Administrator die übernommenen Einstellungen akzeptieren. Alternativ kann ein Administrator mit Rechte eines Umgebungskonfigurations-Administrators eine beliebige Operatorkategorie aktivieren und vererbte Einstellungen auf Umgebungsebene überschreiben.

Um die Einstellungen für eine Operatorkategorie zu prüfen, müssen Sie die Kategorie aktivieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie "Domäne", wählen Sie eine Umgebung aus, und klicken Sie auf "Sperren".
3. Klicken Sie auf die Registerkarte "Module".
4. Um die Einstellungen für Operatorkategorien anzuzeigen, klicken Sie die Einstellung "Von Domäne übernehmen", und wählen Sie "Aktivieren" aus der Drop-down-Liste aus.
5. Klicken Sie mit der rechten Maustaste auf die Operatorkategorie, und wählen Sie "Bearbeiten" aus.

   Die aktuellen Einstellungen werden angezeigt.
6. Optional können Sie Einstellungen für ein oder mehrere Felder konfigurieren.

   Hinweis: Weitere Informationen zur Feldebene finden Sie unter Konfigurieren der Operatorkategorien (siehe Seite 289).
7. Klicken Sie auf "Speichern".
8. Klicken Sie auf "Schließen".
9. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie "Entsperren" aus.

Angeben von Auslösereinstellungen für Umgebungen

Auslösereinstellungen sind auf der Umgebungsebene standardmäßig deaktiviert. Wenn die Auslösereinstellung auf Domänenebene konfiguriert wurde, können Sie angeben, dass Sie diese Einstellungen übernehmen möchten. Alternativ können Sie einen Auslöser aktivieren und anschließend die Einstellungen auf Domänenebene überschreiben. Bei Bedarf können Sie einen Auslöser deaktivieren, der aktiviert ist oder zum Übernehmen von Werten festgelegt ist.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Überprüfen Sie die Einstellungen auf Domänenebene für den Auslöser:
   a. Klicken Sie auf "Domäne"
   b. Klicken Sie auf die Registerkarte "Auslöser".
   c. Doppelklicken Sie auf einen Auslöser.
   d. Überprüfen Sie, ob der Auslöser konfiguriert wurde, und wenn dies der Fall ist, ob die Einstellungen für eine bestimmte Umgebung akzeptiert werden sollen.
3. Wählen Sie eine Umgebung aus, und klicken Sie auf "Sperren".
4. Klicken Sie auf die Registerkarte "Auslöser".
5. Wählen Sie einen Auslöser aus.
6. Wählen Sie einen neuen Wert aus der Drop-down-Liste aus.

   Von Domäne erben

   Gibt an, dass die Einstellungen, die auf Domänenebene konfiguriert sind, in der ausgewählten Umgebung verwendet werden.

   Deaktiviert

   Gibt an, dass dieser Auslöser nicht in dieser Umgebung verwendet wird.

   Aktiviert

   Gibt an, dass dieser Auslöser die für diese Umgebung konfigurierten Einstellungen verwenden soll.
7. Wenn Sie "Aktiviert" auswählen, dann klicken Sie mit der rechten Maustaste auf den Auslöser und wählen Sie "Bearbeiten" aus. Bearbeiten Sie die Einstellungen und verwenden Sie Folgendes als Leitfaden:
   - Konfigurieren der Dateiauslöser-Eigenschaften auf Domänenebene (siehe Seite 341).
   - Konfigurieren von E-Mail-Auslösereigenschaften auf Domänenebene (siehe Seite 343).
   - Konfigurieren von SNMP-Auslösereigenschaften auf Domänenebene (siehe Seite 346).

- Konfigurieren von Catalyst-Auslösereigenschaften auf Domänenebene (siehe Seite 338).

8. Klicken Sie auf "Speichern".
9. Klicken Sie auf "Schließen".
10. Wählen Sie die aktualisierte Umgebung aus, und klicken Sie auf "Entsperren".

Aktualisieren einer Umgebungshierarchie

Die Domänenhierarchie besteht aus einer oder mehreren Umgebungen, wobei jede Umgebung mindestens einen Koordinationsrechner und einen oder mehrere Kontaktpunkte hat, die die Umgebung zu einem Agenten zuordnen. Wenn ein Operator in einem ausgeführten Prozess auf einen Kontaktpunkt verweist, wird dieser Operator auf dem Agenten oder auf dem Koordinationsrechner, der dem Kontaktpunkt zugeordnet ist, ausgeführt. Wenn ein Operator auf eine Kontaktpunktgruppe verweist, wird er auf allen zugeordneten Agenten und Koordinationsrechner ausgeführt.

Um das Ausführen von Operatoren auf Remote-Hosts, die Hosts ohne Agenten sind, zu unterstützen, kann eine Umgebung Proxy-Kontaktpunkte und Hostgruppen einschließen. Ein Proxy-Kontaktpunkt ordnet einen Remote-Host einem Agenten zu. Eine Hostgruppe ordnet einem Agenten viele Remote-Hosts zu. In beiden Fällen stellt der Agentenhost eine vertrauenswürdige SSH-Verbindung zum Remote-Host her.

Ein Administrator mit den Berechtigungen "Environment_Configuration_Admin" (Konfigurationsadministrator) kann die Hierarchie einer ausgewählten Umgebung aktualisieren. Die Kontextmenüoptionen für eine Umgebung:

Neue Gruppe hinzufügen
Kontaktpunkt hinzufügen
Hostgruppe hinzufügen
Entsperren
Sperren
Umbenennen
Gebündelte Entfernung von Kontaktpunkten
Löschen
Aktualisieren

Es folgen Verknüpfungen zu Themen für die Menüoptionen der Umgebung:

- Neue Gruppe hinzufügen

  Weitere Informationen finden Sie unter Gruppieren von Kontaktpunkten in einer Umgebung (siehe Seite 250).

- Kontaktpunkt hinzufügen

  Weitere Informationen finden Sie unter Hinzufügen eines Kontaktpunkts und Erstellen einer Zuordnung (siehe Seite 242). Details finden Sie in den Kapiteln "Verwalten von Kontaktpunkten" und "Verwalten von Proxy-Kontaktpunkten".

  Weitere Informationen finden Sie auch unter Hinzufügen eines Koordinationsrechners zu einer Umgebung (siehe Seite 178).

- Hostgruppe hinzufügen

  Weitere Informationen finden Sie unter Erstellen einer Hostgruppe (siehe Seite 269). Details finden Sie im Kapitel "Verwalten von Hostgruppen".

- Umbenennen

  Weitere Informationen finden Sie unter Umbenennen einer Umgebung (siehe Seite 177).

- Gebündelte Entfernung von Kontaktpunkten

  Weitere Informationen finden Sie unter Gebündeltes Entfernen nicht verwendeter leerer Kontaktpunkte (siehe Seite 248).

- Löschen: Kann verwendet werden, um ein logisches Objekt, das ein Anwender hinzugefügt hat, aus der Domänenhierarchie zu entfernen, das bedeutet:

  - Eine beliebige Umgebung.
  - Ein beliebiger Koordinationsrechner-Kontaktpunkt.

    Weitere Informationen finden Sie unter Löschen eines Koordinationsrechner-Kontaktpunkts (siehe Seite 179).

  - Ein beliebiger Agentenkontaktpunkt.
  - Eine beliebige Kontaktpunktgruppe.
  - Eine beliebige Hostgruppe.

Umbenennen einer Umgebung

Administratoren mit Environment_Configuration_ Admin-Rechten (Konfigurationsadministrator) können eine Umgebung umbenennen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".

   Das Auswahlmenü "Konfigurationsbrowser" ist geöffnet.

2. Klicken Sie mit der rechten Maustaste auf die Domäne, und klicken Sie dann auf "Sperren".
3. Klicken Sie mit der rechten Maustaste auf die Umgebung, und klicken Sie dann auf "Sperren".
4. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie "Umbenennen" aus.
5. Geben Sie einen neuen Namen für die Umgebung ein.
6. Klicken Sie auf "Speichern".
7. Klicken Sie mit der rechten Maustaste auf die Domäne, und klicken Sie dann auf "Entsperren".

Hinzufügen eines Koordinationsrechners zu einer Umgebung

Bei der Erstinstallation von CA Process Automation wird der Domänen-Koordinationsrechner in der Standardumgebung installiert. Die Standardumgebung wird normalerweise für das Entwerfen und Testen verwendet. Oft erstellen Administratoren eine separate Umgebung für die Produktion.

Jede Umgebung muss mindestens einen Koordinationsrechner haben, aber jede Umgebung kann mehrere Koordinationsrechner haben. Jeder neue Koordinationsrechner erfordert eine eigene Installation. Nachdem Sie einen separaten Koordinationsrechner installiert haben, fügen Sie den neu installierten Koordinationsrechner einer Umgebung hinzu.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Klicken Sie mit der rechten Maustaste auf die zu konfigurierende Umgebung, und klicken Sie dann auf "Sperren".
3. Klicken Sie erneut mit der rechten Maustaste auf die Umgebung, und klicken Sie dann auf "Kontaktpunkt hinzufügen".

   Das Dialogfeld "Kontaktpunkt hinzufügen" wird geöffnet.
4. Geben Sie neben "Kontaktpunktname" einen Namen für den neuen Koordinationsrechner ein.
5. Klicken Sie neben "Agenten/Koordinationsrechner auswählen" auf "Koordinationsrechner".

   Die Option "Koordinationsrechner" ist nicht verfügbar, wenn alle Koordinationsrechner in der Domäne bereits vorhandenen Kontaktpunkten zugeordnet sind.
6. Wählen Sie in der Liste der verfügbaren Koordinationsrechner den Koordinationsrechner aus, den Sie dem neuen Kontaktpunkt zuordnen möchten.
7. Klicken Sie auf "Speichern", um den neuen Kontaktpunkt der Umgebung hinzuzufügen.
8. Wählen Sie das Auswahlmenü "Browser" aus, klicken Sie mit der rechten Maustaste auf die Umgebung, und klicken Sie dann auf "Entsperren".

   Durch das Dialogfeld "Nicht gespeicherte Daten" werden Sie aufgefordert, die Änderungen zu speichern.
9. Klicken Sie auf "Ja".

   Hinweis: Sie können die Änderungen auch mithilfe von "Speichern" am oberen Bildschirmrand oder über das Menü "Datei" speichern, ohne die Sperre aufzuheben.

Weitere Informationen:

Hinzufügen eines Kontaktpunkts für einen Koordinationsrechner (siehe Seite 189)

Löschen eines Koordinationsrechner-Kontaktpunkts

Ein Koordinationsrechner-Kontaktpunkt ist eine logische Entität, die einen ausgewählten Koordinationsrechner oder seinen Lastenausgleich einer bestimmten Umgebung zuordnet. Wenn Sie einen Koordinationsrechner-Kontaktpunkt löschen, wird die Zuordnung entfernt, was jedoch keine Auswirkungen auf die Umgebung oder den Koordinationsrechner hat. Auf einen physischen Koordinationsrechner ohne Kontaktpunkt kann allerdings nicht zugegriffen werden. Operatoranfragen oder Aktualisierungen der Bibliothek können nicht akzeptiert werden.

Sie können einen Koordinationsrechner-Kontaktpunkt in Vorbereitung für das Erstellen eines neuen Kontaktpunkts für diesen Koordinationsrechner löschen. Sie können einen Koordinationsrechner-Kontaktpunkt in Vorbereitung für das Deaktivieren dieses Koordinationsrechners löschen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie den Domänenknoten und den Umgebungsknoten mit dem zu entfernenden Koordinationsrechner.
3. Klicken Sie mit der rechten Maustaste auf die Domäne, und klicken Sie dann auf "Sperren".
4. Klicken Sie mit der rechten Maustaste auf die Umgebung, die den Koordinationsrechner enthält, den Sie löschen möchten, und klicken Sie auf "Sperren".
5. Klicken Sie mit der rechten Maustaste auf den zu löschenden Koordinationsrechner, und wählen Sie "Löschen" aus.
6. Klicken Sie auf "OK", um das Löschen des Koordinationsrechners zu bestätigen.
7. Klicken Sie mit der rechten Maustaste auf die Umgebung, und klicken Sie dann auf "Entsperren".
8. Klicken Sie mit der rechten Maustaste auf die Domäne, und klicken Sie dann auf "Entsperren".

   Der Kontaktpunkt "Koordinationsrechner" wird gelöscht.

Kapitel 7: Verwalten von Koordinationsrechnern

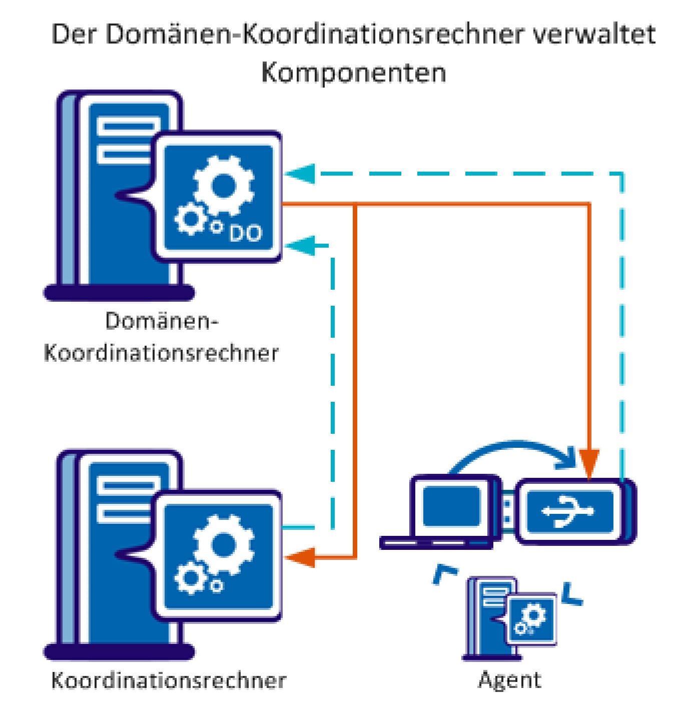
Sie können so viele Koordinationsrechner installieren, wie notwendig ist. Die erste Installation erstellt den Domänen-Koordinationsrechner. Sobald der Domänen-Koordinationsrechner in Betrieb ist, können Sie zusätzliche Koordinationsrechner aus dem Auswahlmenü "Installation" auf der Registerkarte "Konfiguration" installieren.

Koordinationsrechner sind die "Engines" von CA Process Automation; sie verarbeiten den Inhalt, der mit CA Process Automation entworfen wurde. Alle Prozesse werden auf Koordinationsrechnern ausgeführt, die Automatisierungsobjekte verwalten und ausführen. Koordinationsrechner weisen Agenten an, erforderliche Aktionen als Teil des Prozesses auszuführen.

Dieses Kapitel enthält folgende Themen:

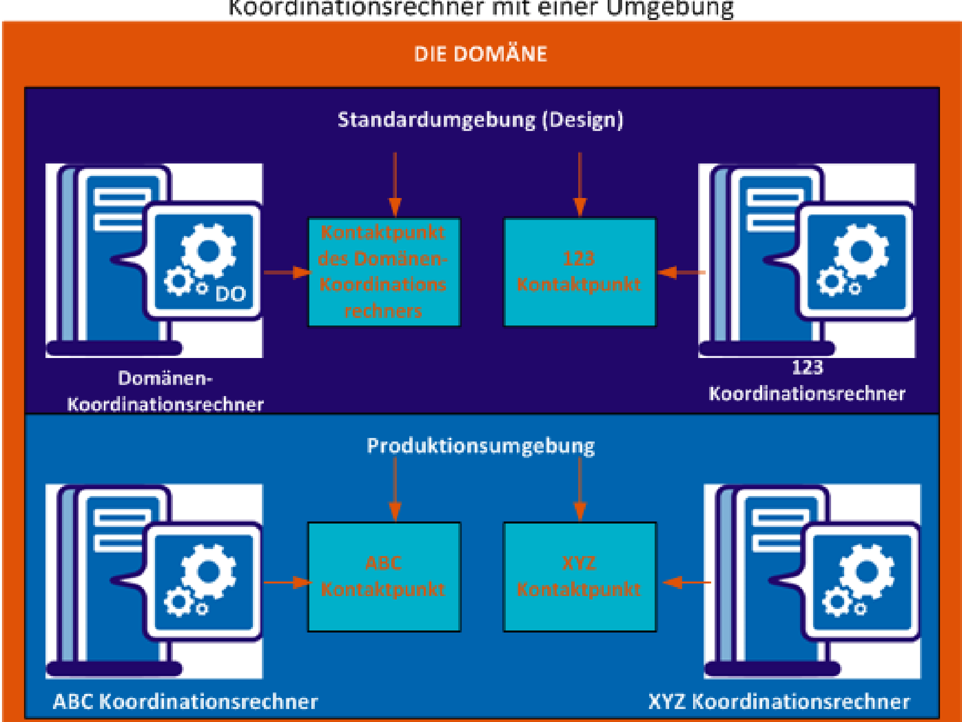
Info zu Koordinationsrechner

Der Domänen-Koordinationsrechner verwaltet die Konfiguration und den Status aller Komponenten in der Domäne. Sie können Aktualisierungen für Koordinationsrechner oder Agenten auf den Domänen-Koordinationsrechner hochladen. Der Domänen-Koordinationsrechner sendet die Aktualisierungen, die Sie hochladen, an alle Koordinationsrechner oder Agenten. Alle Koordinationsrechner und Agenten in der Domäne senden ihren Status regelmäßig an den Domänen-Koordinationsrechner.

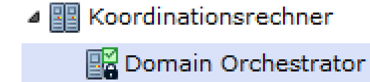


Um einen Koordinationsrechner zu einer Umgebung hinzuzufügen, konfigurieren Sie einen Kontaktpunkt für den ausgewählten Koordinationsrechner in der Umgebung, die Sie angeben. Jeder Koordinationsrechner nimmt nur an einer CA Process Automation-Umgebung teil. Jeder Koordinationsrechner wird einem Kontaktpunkt zugeordnet. Wenn ein Operator auf einem Koordinationsrechner-Kontaktpunkt ausgeführt werden soll, wird das Feld "Ziel" leer gelassen. Ein Feld "Ziel" ohne Eingabe bedeutet, dass der Operator auf dem Koordinationsrechner ausgeführt wird, auf dem der Prozess gestartet wurde.

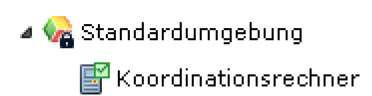
Der Kontaktpunkt eines Koordinationsrechners verbindet den Koordinationsrechner mit einer Umgebung



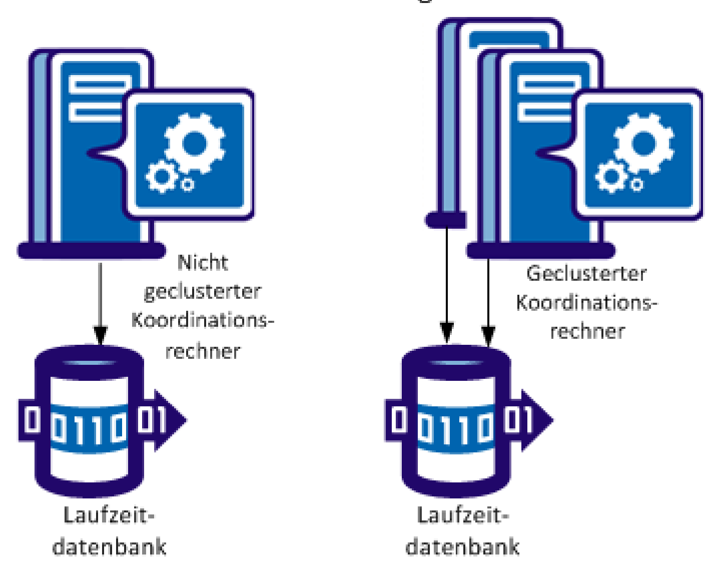
Sie konfigurieren Host-spezifische Einstellungen und zeigen physische Informationen für einen Koordinationsrechner im Knoten Koordinationsrechner an.



Sie konfigurieren kontaktpunktspezifische Einstellungen für den gleichen Koordinationsrechner im Knoten "Umgebung". Sie können logische Informationen zu einem Koordinationsrechner unter seiner Umgebung anzeigen.

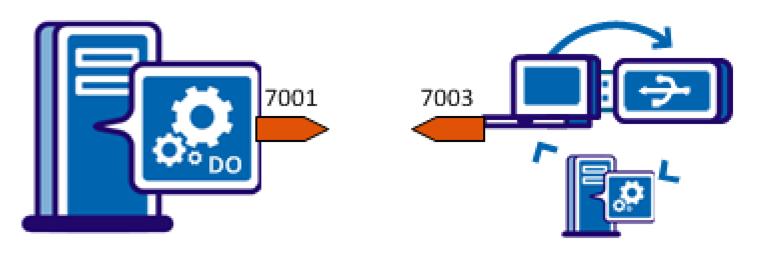


Koordinationsrechner können (mit mehreren Knoten) für Hochverfügbarkeit und Skalierbarkeit *geclustert* oder *nicht geclustert* (mit einem einzelnen Knoten*)* sein. Ein geclusterter Koordinationsrechner agiert als einzelner Koordinationsrechner. Während beispielsweise jeder nicht geclusterte Koordinationsrechner seine eigene Laufzeitdatenbank hat, nutzen die Koordinationsrechner in einem geclusterten Knoten gemeinsam eine Laufzeitdatenbank.

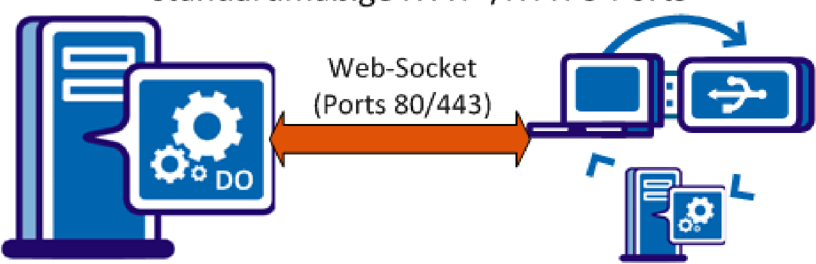


Ein Prozess, der auf einem Koordinationsrechner ausgeführt wird, kann auf einem separaten Koordinationsrechner einen Unterprozess ausführen. Ein Agent kann Schritte in einem Prozess ausführen, zum Beispiel das Ausführen eines Skripts. Koordinationsrechner und Agenten verwenden zwei Ports, um miteinander zu kommunizieren.

Mit veralteten Kommunikationen ist der Standardport für Koordinationsrechner 7001, während der Standardport für Agenten 7003 ist. Port 7001 und Port 7003 sind bidirektional, das heißt, dass Sie Daten sowohl senden als auch empfangen.



Mit vereinfachten Kommunikationen initiieren Agenten eine persistente Web-Socket-Verbindung, die der Agent und der Koordinationsrechner für die Kommunikation verwenden.



Wenn der Koordinationsrechner erfordert, dass ein Agent einen Schritt abschließt, gibt der Agent die Ergebnisse an den Koordinationsrechner zurück. In einem geclusterten Setup sendet ein Koordinationsrechner-Knoten eine Anfrage an einen Agenten. Der Agent sendet das Ergebnis an einen beliebigen Knoten des Koordinationsrechners, der die Anfrage gesendet hat. Einer der Cluster-Knoten nimmt das Agentenergebnis aus der freigegebenen Warteschlange auf.

Konfigurieren der Inhalte eines Koordinationsrechner-Kontaktpunkts

Um einen Koordinationsrechner-Kontaktpunkt zu konfigurieren, wählen Sie diesen Koordinationsrechner unter einem Umgebungsknoten aus. Alle außer einer der Einstellungen ist schreibgeschützt.

Um Einstellungen zu konfigurieren, die zum Koordinationsrechner-Host gehören, wählen Sie den Koordinationsrechner unter dem Knoten "Koordinationsrechner" aus.

Hinweis: Weitere Informationen zur Konfiguration finden Sie unter Konfigurieren der Inhalte eines Koordinationsrechner-Hosts (siehe Seite 192).

Es folgen die Registerkarten für Inhalte des ausgewählten Koordinationsrechners:



Das einzige konfigurierbare Feld auf diese Registerkarten ist das Feld "Kontaktpunktsicherheit". Legen Sie auf der Registerkarte "Eigenschaften" das Feld "Kontaktpunktsicherheit" nur auf "Wahr" fest, nachdem Sie eine Richtlinie zur Kontaktpunktsicherheit konfiguriert haben.

Es folgen Themen für die Registerkarte "Koordinationsrechner":

- Sicherheit: Sicherheitseinstellungen gelten nicht für den Koordinationsrechner-Kontaktpunkt. Die Felder sind in der Ansicht des Koordinationsrechner-Kontaktpunkts schreibgeschützt.
- Eigenschaften: Sie können Eigenschaften eines Koordinationsrechner-Kontaktpunkts konfigurieren (siehe Seite 186).
- Module: Operatorkategorien können von einem Koordinationsrechner-Kontaktpunkt aus nicht konfiguriert werden. Sie können Einstellungen bearbeiten, indem Sie den Koordinationsrechner-Host auswählen.
- Auslöser: Auslöser können von einem Koordinationsrechner-Kontaktpunkt aus nicht konfiguriert werden. Sie können Einstellungen bearbeiten, indem Sie den Koordinationsrechner-Host auswählen.
- Richtlinien: Richtlinien können von einem Koordinationsrechner-Kontaktpunkt aus nicht konfiguriert werden. Sie können Einstellungen bearbeiten, indem Sie den Koordinationsrechner-Host auswählen.
- Spiegelung: Spiegelung kann von einem Koordinationsrechner-Kontaktpunkt aus nicht konfiguriert werden. Sie können die Spiegelungseinstellung bearbeiten, indem Sie den entsprechenden Koordinationsrechner-Host auswählen.
- Audit-Pfade: Aktionen der Audit-Pfade gelten nicht für Koordinationsrechner-Kontaktpunkte. Sie können Aktionen anzeigen, für die auf den entsprechenden Koordinationsrechner ein Audit durchgeführt wurde.

Konfigurieren der Eigenschaften eines Koordinationsrechner-Kontaktpunkts

Der Eigenschaftsbereich des Koordinationsrechner-Kontaktpunkts stellt Information zum Kontaktpunkt bereit, der dem Koordinationsrechner zugeordnet ist. Sie können Statusinformationen anzeigen und die Konfiguration der Kontaktpunktsicherheit für diesen Koordinationsrechner-Kontaktpunkt ändern.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie die Domäne und die Umgebung mit dem Koordinationsrechner-Kontaktpunkt.
3. Wählen Sie den Koordinationsrechner-Kontaktpunkt aus, der konfigurieret werden soll, und klicken Sie auf Sperren.
4. Klicken Sie auf die Registerkarte Eigenschaften.

5. (Optional) Konfigurieren Sie die Einstellung für Kontaktpunktsicherheit. Geben Sie an, ob Sie die Einstellung erben oder den Wert auf der Ebene des Koordinationsrechners festlegen möchten. Wenn die Einstellung aktiviert ist, verwenden Prozesse die Richtlinien für Kontaktpunktsicherheit, um Anwender dafür zu autorisieren, Operatoren in einem Prozess auszuführen.

6. Konfigurieren Sie die Standardeinstellungen, um festzulegen, wie Operatoren IP-Adressen oder Hostnamen im Feld "Ziel" oder bei Referenzierung durch einen Datensatz verarbeiten sollen.

   a. Die Auswahl Ziel nur in Hostgruppen abgleichen? in der Drop-down-Liste gibt den Suchumfang für ein Operatorziel an, wenn die Eingabe im Feld "Ziel" eine IP-Adresse oder ein Hostname (FQDN) ist. Die Ausführung des Operators auf dem Ziel kann nur fortfahren, wenn das Ziel CA Process Automation bekannt ist.

      - Wählen Sie "Deaktiviert" aus, um eine möglichst umfassende Suche zu ermöglichen.

      - Wählen Sie hier Aktiviert und für das nächste Feld "Deaktiviert" aus, um die Suche möglichst eingeschränkt zu gestalten.

   b. Wenn die Drop-down-Liste "Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen?" aktiviert ist, geben Sie an, ob die Suche durch Hostgruppen-Referenzen auf den Eingabetyp beschränkt werden soll.

      - Wählen Sie Aktiviert aus, um alle Hostgruppen-Referenzen in die Suche einzubeziehen.

      - Wählen Sie Deaktiviert aus, um die Suche auf Hostgruppen-Referenzen zu beschränken, die eine genaue Übereinstimmung mit der Eingabe im Feld "Ziel" enthalten.

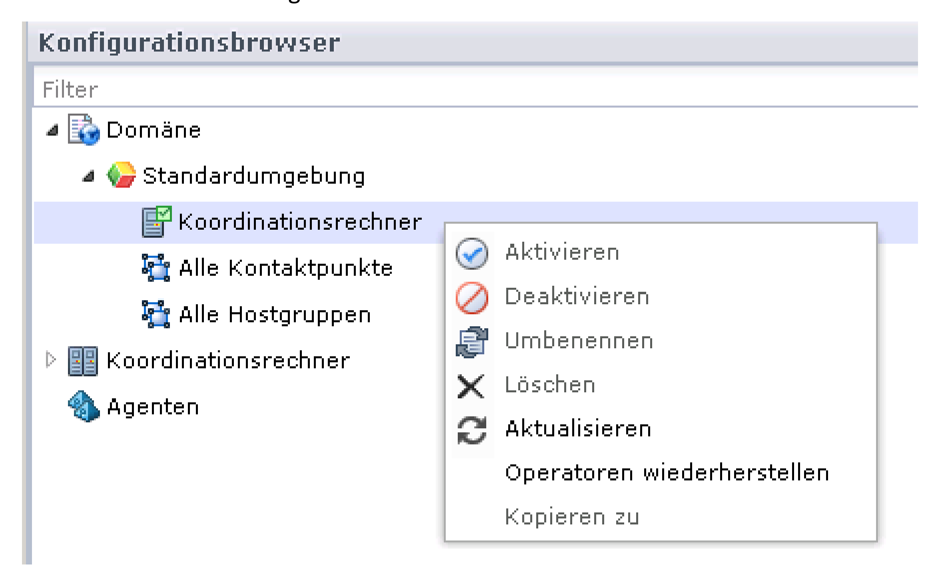
7. Klicken Sie auf "Speichern".

8. Wählen Sie den Koordinationsrechner aus, und klicken Sie auf "Entsperren".

9. Zeigen Sie die Informationseigenschaften an. Weitere Informationen finden Sie in den QuickInfos.

Aktualisieren der Hierarchie eines Koordinationsrechner-Kontaktpunkts

Wenn Sie einen Koordinationsrechner unter "Domäne" bzw. "Umgebung" auswählen, sind die angezeigten Details für den Kontaktpunkt relevant, der diesem Koordinationsrechner zugeordnet ist.



Sehen Sie sich Folgendes an:

- Aktivieren: Klicken Sie mit der rechten Maustaste auf einen deaktivierten Koordinationsrechner-Kontaktpunkt, und wählen Sie "Aktivieren" aus.
- Deaktivieren

  Weitere Informationen finden Sie unter Deaktivieren eines Koordinationsrechner-Kontaktpunkts (siehe Seite 191).
- Umbenennen: Geben Sie einen neuen Namen für den Koordinationsrechner-Kontaktpunkt an.
- Löschen: Klicken Sie mit der rechten Maustaste auf einen Koordinationsrechner-Kontaktpunkt, und wählen Sie "Löschen" aus. Nur der Kontaktpunkt wird gelöscht.
- Operatoren wiederherstellen

  Weitere Informationen finden Sie unter Wiederherstellen von Operatoren auf dem Ziel-Koordinationsrechner (siehe Seite 190).
- Kopieren zu

  Weitere Informationen finden Sie unter Erstellen einer Kontaktpunktgruppe mit ausgewählten Kontaktpunkten (siehe Seite 252)

Hinzufügen eines Kontaktpunkts für einen Koordinationsrechner

Wenn Sie einen eigenständigen Koordinationsrechner zu einer Umgebung hinzufügen, fügen Sie einen Kontaktpunkt zu der Umgebung hinzu, und ordnen Sie ihm diesen Koordinationsrechner zu. Jeder Koordinationsrechner muss mit einem eigenen Kontaktpunkt verbunden sein.

Wenn Sie Knoten hinzufügen, um einen geclusterten Koordinationsrechner zu erstellen, verwendet der Lastenausgleich den Kontaktpunkt, den Sie für den ersten Knoten definiert haben. Der Lastenausgleich bestimmt, welcher Knoten eine Anfrage verarbeitet, die auf den Kontaktpunkt abzielt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie mit der rechten Maustaste auf die Umgebung, zur der ein Kontaktpunkt hinzugefügt werden soll, und klicken Sie auf "Sperren".
3. Erweitern Sie den Knoten "Koordinationsrechner".
4. Klicken Sie mit der rechten Maustaste auf den Ziel-Koordinationsrechner, wählen Sie "Kontaktpunkt konfigurieren in" aus, und klicken Sie auf den Namen der Umgebung, die Sie gesperrt haben.
5. Geben Sie im Dialogfeld "Koordinationsrechner-Kontaktpunkt hinzufügen" einen Namen für den neuen Kontaktpunkt ein, und klicken Sie auf "Hinzufügen".
6. Klicken Sie mit der rechten Maustaste auf die Umgebung, in der Sie den Kontaktpunkt hinzugefügt haben, und wählen Sie Entsperren aus.

   Im Dialogfeld Nicht gespeicherte Daten werden Sie aufgefordert, die Änderungen zu speichern.
7. Klicken Sie auf Ja.

   Der ausgewählten Umgebung wird ein neuer Koordinationsrechner-Kontaktpunkt hinzugefügt.

Weitere Informationen:

Hinzufügen eines Koordinationsrechners zu einer Umgebung (siehe Seite 178)

Wiederherstellen von Operatoren auf dem Ziel-Koordinationsrechner

Die manuelle Wiederherstellung ist stets aktiviert. Sie können "Operatoren wiederherstellen" unabhängig davon aufrufen, ob die Option "Automatische Operator-Wiederherstellung" auf Zielebene auf "Wahr", "Falsch" oder "Von Umgebung übernehmen" festgelegt ist. Die Operator-Wiederherstellung ist geeignet, wenn sich ein Prozess im Zustand "Blockiert", "Wird ausgeführt" oder "Im Wartezustand" befindet und ein Operator im Prozess mit einem Systemfehler fehlschlägt. Bei der Operator-Wiederherstellung wird der Operator zurückgesetzt, und anschließend wird der Prozess fortgesetzt.

Sie können die Operator-Wiederherstellung in den folgenden Fällen mit der Registerkarte "Konfiguration" aufrufen:

- Der zuvor inaktive Koordinationsrechner wird aktiv. Ein aktiver Koordinationsrechner wird grün angezeigt.
- Der Ziel-Koordinationsrechner wird aktiviert.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie die Domäne und eine Umgebung, in der ein Koordinationsrechner über einen oder mehrere Prozesse verfügt, für die festgelegt wurde, dass sie wiederherstellbar sind.
3. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, und wählen Sie Aktualisieren aus.
4. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, und wählen Sie Operatoren wiederherstellen aus.

   Die Operator-Wiederherstellung startet.

Deaktivieren eines Koordinationsrechner-Kontaktpunkts

Deaktivieren Sie einen Koordinationsrechner-Kontaktpunkt, um zu verhindern, dass Prozesse auf diesem Koordinationsrechner-Kontaktpunkt ausgeführt werden. Das Deaktivieren eines Koordinationsrechner-Kontaktpunkts wirkt sich nicht auf die Koordinationsrechner-Bibliothek aus. Das heißt, Designer können einen Koordinationsrechner mit einem deaktivierten Kontaktpunkt auf der Registerkarte "Bibliothek" auswählen und Automatisierungsobjekte definieren.

Sie deaktivieren einen Koordinationsrechner-Kontaktpunkt, wenn betroffene externe Objekte nicht verfügbar sind. Berücksichtigen Sie das Beispiel für Prozesse, die mit Service Desk oder mit einer externen Datenbank arbeiten. Zu bestimmten Zeiten sind diese Komponenten aufgrund von Wartung nicht verfügbar. Sie können verhindern, dass Prozesse ausgeführt werden, die mit vorübergehend nicht verfügbaren Komponenten interagieren. Wenn die externen Komponenten verfügbar sind, aktivieren Sie den Koordinationsrechner-Kontaktpunkt. Dann können geplante Prozesse, die diese externen Komponenten verwenden, erneut ausgeführt werden.

Sie können den Koordinationsrechner-Kontaktpunkt deaktivieren, den Sie auf der Domänenhierarchie auswählen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie den Knoten "Domäne". Erweitern Sie den Umgebungsknoten mit dem zu deaktivierenden Koordinationsrechner-Kontaktpunkt.
3. Wählen Sie die Umgebung aus, und klicken Sie auf "Sperren".
4. Wählen Sie den Koordinationsrechner-Kontaktpunkt aus, und klicken Sie auf "Sperren".
5. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner-Kontaktpunkt, und wählen Sie "Deaktivieren" aus.
6. Klicken Sie auf "Entsperren".
7. Klicken Sie auf die gesperrte Umgebung, und klicken Sie auf "Entsperren".

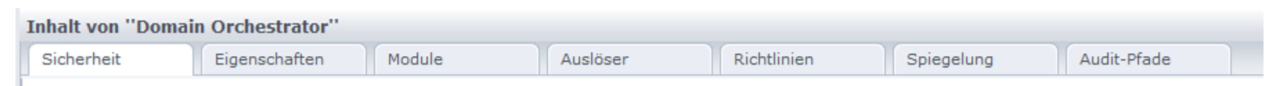
Weitere Informationen:

Festlegen der Quarantäne für einen Koordinationsrechner (siehe Seite 204)

Konfigurieren der Inhalte eines Koordinationsrechner-Hosts

Konfigurationsdetails, die ausschließlich für den Koordinationsrechner und nicht vererbt sind, beinhalten Richtlinien und Spiegelungen, die Standardwerte für alle Felder haben. Spiegelung gilt für Koordinationsrechner, mit Ausnahme des Domänen-Koordinationsrechners. Folgende Einstellungen werden standardmäßig übernommen: Sicherheit, Eigenschaften, Module und Auslöser. Die Einstellungen, die Sie für einen Koordinationsrechner-Host konfigurieren, unterscheiden sich von den Einstellungen, die Sie auf dem Koordinationsrechner-Kontaktpunkt konfigurieren.

Es folgen die Registerkarten für das Menü "Koordinationsrechner-Host":



- Sicherheit

  Weitere Informationen finden Sie unter Anzeigen der Sicherheitseinstellungen des Koordinationsrechners (siehe Seite 193).

- Eigenschaften

  Weitere Informationen finden Sie unter Eigenschaften eines Koordinationsrechner-Kontaktpunkts (siehe Seite 186).

- Module

  Weitere Informationen finden Sie unter Überschreiben der von der Umgebung übernommenen Einstellungen der Operatorkategorie (siehe Seite 197).

- Auslöser

  Weitere Informationen finden Sie unter Aktivieren von Auslösern für einen Koordinationsrechner (siehe Seite 198).

- Richtlinien

  Weitere Informationen finden Sie unter Konfigurieren der Koordinationsrechner-Richtlinien (siehe Seite 199).

- Spiegelung

  Weitere Informationen finden Sie unter Konfigurieren der Koordinationsrechner-Spiegelung (siehe Seite 202).

- Audit-Pfade

  Weitere Informationen finden Sie unter Anzeigen des Audit-Pfads für einen Koordinationsrechner (siehe Seite 362).

Anzeigen der Sicherheitseinstellungen des Koordinationsrechners

Die meisten Einstellungen der Registerkarte "Sicherheit" werden während des Installationsprozesses des Domänen-Koordinationsrechners erstellt. Sie können keine dieser Einstellungen über die Benutzeroberfläche ändern. Sie können diese Einstellungen ändern, indem Sie den Domänen-Koordinationsrechner neu installieren.

Das Kontrollkästchen "Erben" bezieht sich nur auf Aktualisierungsintervall der CA EEM-Cache-Aktualisierung (in Sekunden). Sie können das Aktualisierungsintervall kürzen, wenn Sie möchten, dass CA Process Automation die von Ihnen in CA EEM durchgeführten Änderungen schneller erhält.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie im Auswahlmenü "Konfigurationsbrowser" die Option "Koordinationsrechner".
3. Wählen Sie einen Koordinationsrechner aus. Sie können Sicherheitseinstellungen auf der Registerkarte "Sicherheit" anzeigen.
4. Um die Einstellungen zu aktualisieren:
   a. Klicken Sie auf Sperren.
   b. Deaktivieren Sie das Kontrollkästchen Erben.
   c. Aktualisieren Sie den Wert für Aktualisierungsintervall der CA EEM-Cache-Aktualisierung (in Sekunden).
   d. Klicken Sie auf "Speichern".
   e. Klicken Sie auf Entsperren.

Konfigurieren der Hosteigenschaften des Koordinationsrechners

Sie können Hosteigenschaften für einen ausgewählten Koordinationsrechner konfigurieren und schreibgeschützte Informationen anzeigen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie den Knoten "Koordinationsrechner".
3. Wählen Sie den Koordinationsrechner aus, der konfiguriert werden soll, und klicken Sie auf Sperren.

4. Klicken Sie auf die Registerkarte "Eigenschaften", und zeigen Sie die schreibgeschützten Eigenschaftseinstellungen des Koordinationsrechners an:
   - Domäne
   - Hostname
   - Koordinationsrechner-Name
   - Status
5. Konfigurieren Sie folgende Felder:

   Automatische Operator-Wiederherstellung

   Gibt an, ob die Wiederherstellung automatisiert werden soll. Die Wiederherstellung gilt für Operatoren, die mit einem SYSTEM_ERROR-Fehler fehlschlagen und deren wiederherstellbare Prozesse sich im Zustand "Blockiert", "Wird ausgeführt" oder "Im Wartezustand" befinden, wenn die Wiederherstellung ausgelöst wird. Wenn die automatische Wiederherstellung festgelegt wird, initiiert jeder Koordinationsrechner innerhalb der Umgebung die Wiederherstellung automatisch, wenn der Koordinationsrechner wieder aktiv wird. Bei der Wiederherstellung werden die betroffenen Prozesse gestartet, und die Ausführung ihrer Operatoren auf diesem Koordinationsrechner beginnt.

   Werte: Diese Eigenschaft hat folgende Werte:

   - **Von Umgebung erben**: Den Wert verwenden, der für dieses Feld in den Umgebungseigenschaften konfiguriert ist.
   - **Wahr**: Die Wiederherstellung wird automatisiert.
   - **Falsch**: Die automatische Wiederherstellung wird verhindert.

   Standard: Von Umgebung erben.

Ziel nur in Hostgruppen abgleichen?

Gibt den Suchbereich für ein Operatorziel an, wenn die Eingabe im Feld "Ziel" eine IP-Adresse oder ein Hostname (FQDN) ist. Die Ausführung des Operators auf dem Ziel kann nur fortfahren, wenn das Ziel CA Process Automation bekannt ist. Wählen Sie "Deaktiviert" aus, um eine möglichst umfassende Suche zu ermöglichen. Wählen Sie hier "Aktiviert" und für das nächste Feld "Deaktiviert" aus, um die Suche möglichst eingeschränkt zu gestalten.

Hinweis: Eine DNS-Suche mit einem angegebenen Hostnamen findet zugeordnete IP-Adressen; eine DNS-Suche mit der IP-Adresse findet zugeordnete Hostnamen.

Werte: Diese Eigenschaft hat folgende Werte:

- **Von Umgebung erben**: Den Wert verwenden, der für dieses Feld in den Umgebungseigenschaften konfiguriert ist.
- **Aktiviert**: Der Bereich der Suche hängt davon ab, ob das Feld "Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen" aktiviert oder deaktiviert ist.

  Wenn eine DNS-Suche deaktiviert ist - Suche: Hostgruppe verweist auf einen Remote-Host (exakte Übereinstimmung)

  Wenn eine DNS-Suche aktiviert ist - Suche: Hostgruppe verweist auf einen Remote-Host (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)
- **Deaktiviert**: Die Domänenkomponenten werden in der folgenden Reihenfolge durchsucht:

  Kontaktpunkt (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Koordinationsrechner (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Agent (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Ein Proxy-Kontaktpunkt, der zu einem Remote-Host zugeordnet ist (exakte Übereinstimmung oder Ergebnis einer DNS-Suche)

  Hostgruppenreferenz auf einen Remote-Host (exakte Übereinstimmung oder Ergebnis der DNS-Suche)

Standard: Von Umgebung erben.

Beim Abgleichen von Zielen in Hostgruppen nach DNS suchen?

Hinweis: Dieses Feld wird aktiviert, wenn "Ziel nur in Hostgruppen abgleichen" auf "Aktiviert" gesetzt ist.

Gibt an, ob das Durchsuchen von Hostgruppenreferenzen auf einen Eingabetyp beschränkt werden soll. Zum Beispiel: Wenn der Feld Eingabetyp im Feld "Ziel" ein FQDN ist, wird nur nach Namensmustern für Hosts gesucht. Wenn der Feld Eingabetyp im Feld "Ziel" eine IP-Adresse ist, wird nur nach Teilnetzen gesucht. Wenn eine DNS-Suche eingeschlossen ist, kann die Suche gemäß der Auflösung durch die DNS-Suche auch Hostgruppenreferenzen auf den anderen Typ akzeptieren.

Werte: Diese Eigenschaft hat folgende Werte:

- **Von Umgebung erben**: Den Wert verwenden, der für dieses Feld in den Umgebungseigenschaften konfiguriert ist.
- **Aktiviert**: Alle Hostgruppenreferenzen werden durchsucht. Hostgruppenreferenzen für Hostnamen sind Muster (reguläre Ausdrücke), die den angegebenen Hostnamen enthalten können. Hostgruppenreferenzen für IP-Adressen sind IP-Adressteilnetze, die in CIDR-Notationen ausgedrückt werden, die die angegebene IP-Adresse enthalten können. Dehnen Sie die Suche auf alle Hostgruppenreferenzen aus. Legen Sie fest, ob die Suche eine genaue Übereinstimmung oder eine Übereinstimmung mit dem Ergebnis der DNS-Suche finden soll.
- **Deaktiviert:** Schränkt die Suche auf Hostgruppenreferenzen ein, die eine genaue Übereinstimmung mit der Eingabe im Feld "Ziel" enthalten.

Standard: Von Umgebung erben.

6. Klicken Sie auf "Speichern".
7. Klicken Sie auf Entsperren.

Überschreiben der von der Umgebung übernommenen Einstellungen der Operatorkategorie

Einstellungen der Operatorkategorien werden auf der Registerkarte "Module" konfiguriert. Einstellungen der Operatorkategorie, die auf Umgebungsebene konfiguriert oder von auf Domänenebene konfigurierten Einstellungen übernommen wurden, werden als "Von Umgebung übernehmen" angezeigt. Ein Administrator mit Rechte eines Umgebungskonfigurations-Administrators kann eine beliebige Operatorkategorie aktivieren und vererbte Einstellungen auf Koordinationsrechnerebene überschreiben.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie das Auswahlmenü "Koordinationsrechner".
3. Wählen Sie den Koordinationsrechner aus, den Sie konfigurieren möchten, und klicken Sie auf "Sperren".
4. Klicken Sie auf die Registerkarte "Module".
5. Wählen Sie eine Operatorkategorie aus, klicken Sie auf "Von Umgebung übernehmen", und wählen Sie "Aktivieren" aus der Drop-down-Liste aus.

   Hinweis: Sie können eine Operatorkategorie auf der Koordinationsrechnerebene deaktivieren, indem Sie "Deaktivieren" aus der Drop-down-Liste auswählen.
6. Klicken Sie mit der rechten Maustaste auf die Operatorkategorie, und wählen Sie "Bearbeiten" aus.

   Die Einstellungen werden angezeigt.
7. Ändern Sie eine oder mehrere übernommene Einstellungen.

   Hinweis: Weitere Informationen finden Sie unter Konfigurieren der Operatorkategorien (siehe Seite 289).
8. Klicken Sie auf "Speichern" und "Schließen".

   Die Werte, die im geöffneten Dialogfeld konfiguriert sind, werden gespeichert.
9. Klicken Sie in der Symbolleiste auf die Schaltfläche "Speichern".

   Die gespeicherten Änderungen werden auf die CA Process Automation-Konfiguration angewendet.
10. Wiederholen Sie Schritt 5 bis 9 für jede Operatorkategorie, die Sie aktualisieren möchten.
11. Wählen Sie den konfigurierten Koordinationsrechner aus, und klicken Sie auf "Entsperren".

Aktivieren von Auslösern für einen Koordinationsrechner

Ein Administrator mit Umgebungskonfigurationsrechten kann Auslöser auf Koordinationsrechnerebene verwalten. Sie aktivieren einen ausgewählten Auslöser, indem Sie seinen Status auf "Von Umgebung übernehmen" oder auf "Aktiviert" ändern und die angezeigten Einstellungen überschreiben. Um die aktuellen Einstellungen eines Auslösers anzuzeigen, müssen Sie den Status in "Aktiviert" ändern und "Bearbeiten" auswählen. Wenn Sie die Einstellungen übernehmen, konfigurieren Sie den Auslöser zu "Von Umgebung übernehmen". Wenn Sie die Einstellungen nicht übernehmen, weil sie unvollständig oder für diesen Koordinationsrechner nicht geeignet sind, können Sie die Felder konfigurieren und den Status "Aktiviert" beibehalten.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie das Auswahlmenü "Koordinationsrechner".
3. Klicken Sie mit der rechten Maustaste auf den ausgewählten Koordinationsrechner, und wählen Sie "Sperren" aus.
4. Klicken Sie auf die Registerkarte "Auslöser".

   Wenn keine Auslöser auf der Koordinationsrechnerebene konfiguriert wurden, befinden sie sich im Status "Deaktiviert".

5. Klicken Sie mit der rechten Maustaste auf den zu prüfenden Auslöser, und klicken Sie auf "Bearbeiten".

   Die Felder werden mit den Werten angezeigt, die Sie so verwenden oder ändern können.

6. Wenn der Auslöser vollständig mit Werten konfiguriert ist, die der ausgewählte Koordinationsrechner verwenden soll, wählen Sie "Von Umgebung übernehmen" aus der Drop-down-Liste "Aktivieren/Deaktivieren" aus, und klicken Sie auf "Schließen".

7. Wenn der Auslöser nicht vollständig konfiguriert ist oder wenn Sie verschiedene Werte für den ausgewählten Koordinationsrechner angeben möchten, gehen Sie folgendermaßen vor:

   a. Wählen Sie "Aktiviert" aus der Drop-down-Liste "Aktivieren/Deaktivieren".

   b. Weitere Informationen zu Feldbeschreibungen und andere wichtige Informationen zu allen Auslösern finden Sie unter Verwalten von Auslösern (siehe Seite 335).

   c. Wenn der ausgewählte Auslöser der E-Mail-Auslöser ist und der Koordinationsrechner nicht der Domänen-Koordinationsrechner ist, klicken Sie auf "Durchsuchen", und wählen Sie die Standardprozessdatei aus.

      Das Feld "Standardmäßiger Auslöserprozess" wird mit dem richtigen Pfad für diesen Koordinationsrechner aufgefüllt.

   d. Klicken Sie auf "Schließen".

8. Klicken Sie auf "Speichern".

9. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, den Sie gesperrt haben, und klicken Sie dann auf "Entsperren".

Konfigurieren der Koordinationsrechner-Richtlinien

Die Einstellungen der Koordinationsrechner-Richtlinien geben Verlaufseinstellungen für Prozesse an, die auf dem Koordinationsrechner ausgeführt werden. Sie geben auch den Standardablaufplan und den Standardprozess in der Bibliothek an. Sie können getrennte Richtlinien für getrennte Koordinationsrechner konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.

2. Wählen Sie im Konfigurationsbrowser den Koordinationsrechner aus, den Sie konfigurieren möchten, und klicken Sie auf Sperren.

3. Klicken Sie auf die Registerkarte "Richtlinien".
4. Wählen Sie aus, ob Anwender bearbeitete Objekte beim Einchecken als die gleiche Version speichern können, oder ob die Objektversionskontrolle automatisiert und beim Einchecken eine neuen Version erstellt werden soll.
5. Wenn Sie einen Prozess definiert haben, der standardmäßige Prozess-Handler mit Regeln für das Ändern von Prozessspuren und Handhaben von Ausnahmen angibt, navigieren Sie zu diesem Prozess, und wählen Sie ihn aus.
6. Geben Sie Anforderungen an, um Instanzen von Prozessen, die ausgeführt wurden, beizubehalten.
   a. Wählen Sie die Anzahl von Tagen aus, während der Prozessinstanzen gespeichert werden sollen, die auf einem Kontaktpunkt oder Remote-Host ausgeführt wurden. Wenn Sie einen Tag konfigurieren, bleibt der Prozess mindestens 24 Stunden lang in der Bibliothek, bevor er archiviert wird.
   b. Wählen Sie die Mindestanzahl fehlgeschlagener Instanzen eines Prozesses aus, die im Verlauf beibehalten werden sollen.
   c. Wählen Sie die Mindestanzahl abgeschlossener Instanzen des Prozessobjekts aus, die im Verlauf beibehalten werden sollen.
   d. Wählen Sie die Höchstanzahl der Protokollmeldungen aus, die angezeigt werden können, wenn die Prozessinstanz von einer Prozessüberwachung geöffnet wird.
7. Wählen Sie die Mindestanzahl von Tagen aus, während der ein Anhang in der CA Process Automation-Datenbank gespeichert wird, bevor er gelöscht wird.

   Anwender können Webservices verwenden, um Prozesse auszulösen. Ein Anwender kann direkt einen Prozess starten oder ein Startauftragsformular planen. Anwender können Dateien als Anhänge in den Webservices-Aufrufen senden. Wenn ein Webservice-Aufruf einen Prozess auslöst, können Anwender auf die Dateien in diesem Prozess zugreifen. Ein Anwender kann den SOAP-Operator verwenden, um einen Anhang an den ausgehenden Webservices-Aufruf weiterzuleiten.

8. Geben Sie Anforderungen für das Bereinigen von Prozessinstanzen an, die auf dem ausgewählten Koordinationsrechner ausgeführt und anschließend archiviert wurden. Alternativ können Sie Prozessinstanzen bereinigen, die auf Anfrage innerhalb eines angegebenen Datenbereichs gestartet wurden.

   a. Definieren Sie eine Richtlinie für das Bereinigen archivierter Daten. Es sind folgende Optionen verfügbar:

      Archivierte Daten nicht bereinigen

      Archivierte Prozessinstanzen werden beibehalten, bis sie manuell bereinigt werden.

      Archivierte Daten täglich bereinigen

      Bereinigen Sie archivierte Prozessinstanzen als geplante Aufgabe entsprechend den Einstellungen in den beiden folgenden Feldern.

      Daten ohne Archivierung bereinigen

      Die Prozessinstanzen werden über einen konfigurierten Zeitraum hinweg als aktiv beibehalten. Wenn dieser Zeitraum abgelaufen ist, werden die Daten bereinigt. Es werden keine Prozessinstanzen archiviert.

   b. Definieren Sie den Zeitpunkt (im Format "hh:mm") für das Bereinigen der archivierten Instanzen, die während der konfigurierten Anzahl von Tagen beibehalten wurden.

   c. Definieren Sie die Anzahl von Tagen, während der archivierte Prozessinstanzen beibehalten werden sollen. Nachdem eine archivierte Instanz die konfigurierte Anzahl von Tagen beibehalten worden ist, wird sie um die angegebene Zeit bereinigt.

   d. Um archivierte Instanzen zu bereinigen, die innerhalb eines angegebenen Altersbereichs gestartet wurden, klicken Sie im aktuellen Koordinationsrechner auf die Schaltfläche "Archivierte Instanz löschen", wählen Sie einen Datumsbereich aus, und klicken Sie auf "OK".

9. Geben Sie an, ob Authentifizierung erforderlich ist, wenn ein Anwender versucht, auf Anhänge außerhalb von CA Process Automation zuzugreifen. Wenn dies ausgewählt ist, müssen Anwender gültige Anmeldeinformationen angeben, um auf Anhänge zuzugreifen.

10. Geben Sie an, ob Laufzeitsicherheit durchgesetzt werden soll. Wenn dies ausgewählt ist, wird Laufzeitsicherheit für Prozesse aktiviert, die auf "Aktivieren" gesetzt sind oder diese Einstellung erben.

    Hinweis: Wenn Sie hier die Option "Laufzeitsicherheit aktivieren" auswählen und für einen Prozess die Laufzeitsicherheitsoption "Als Verantwortlicher ausführen" auswählen, verwenden Sie "Verantwortlichen festlegen", um den Besitz der einzelnen betroffenen Prozessobjekte festzulegen. Weitere Informationen finden Sie in der Online-Hilfe oder im *Handbuch für Inhaltsdesign*.

11. Klicken Sie auf "Speichern".

12. Klicken Sie auf Entsperren.

Konfigurieren der Koordinationsrechner-Spiegelung

Koordinationsrechner spiegeln Daten und Konfigurationsinformationen, die auf dem Domänen-Koordinationsrechner gespeichert sind. Die Spiegeleinstellung gibt an, wie oft ein Koordinationsrechner auf Änderungen auf dem Domänen-Koordinationsrechner prüft. Änderungen am Domänen-Koordinationsrechner werden auf den Koordinationsrechner auf dem lokalen Host angewendet. Sie können das Spiegelungsintervall für einen Koordinationsrechner festlegen.

Wenn Sie einen geclusterten Koordinationsrechner auswählen, wird das von Ihnen festgelegte Intervall auf die Spiegelung aller aktiven Knoten im Cluster angewendet. Ein Cluster-Knoten kann inaktiv sein, wenn andere Knoten im Cluster aktualisiert werden. In diesem Fall tritt die Spiegelung für den inaktiven Knoten auf, wenn er gestartet wird.

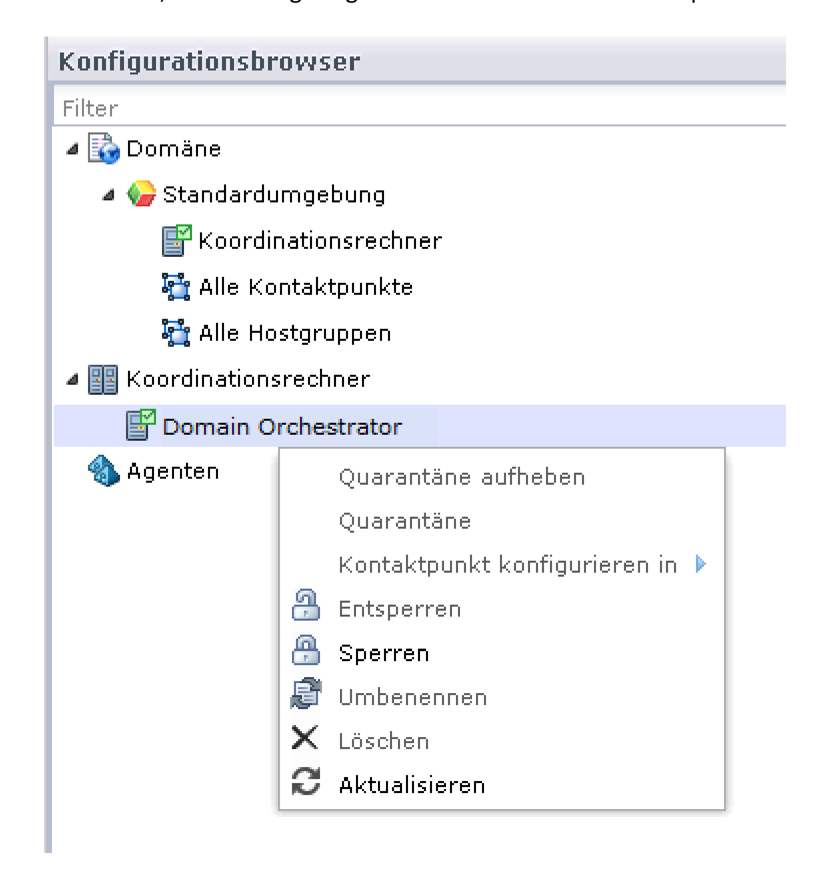
Hinweis: Sie können eine JAR-Datei zum Ordner "Koordinationsrechnerressourcen" auf dem Domänen-Koordinationsrechner hochladen. Wenn Sie den Domänen-Koordinationsrechner neu starten, stellt CA Process Automation die Datei für den Domänen-Koordinationsrechner bereit. Der Domänen-Koordinationsrechner spiegelt (kopiert) die Datei an dem konfigurierten Spiegelungsintervall wider, nach dem Sie die anderen Koordinationsrechner neu starten. Wenn die Koordinationsrechner neu starten, wird die gespiegelte Datei zur Verwendung verfügbar.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie im Auswahlmenü "Konfigurationsbrowser" die Option "Koordinationsrechner".
3. Wählen Sie den zu konfigurierenden Koordinationsrechner aus, und klicken Sie auf "Sperren".
4. Klicken Sie auf die Registerkarte Spiegelung.
5. Wählen Sie im Feld "Spiegelungsintervall (Minuten)" das Intervall aus, in dem die ausgewählten Koordinationsrechner den Domänen-Koordinationsrechner nach Aktualisierungen abfragen sollen. Das Produkt spiegelt Änderungen am ausgewählten Koordinationsrechner im angegebenen Intervall.
6. Klicken Sie auf "Speichern".
7. Wählen Sie im Auswahlmenü "Konfigurationsbrowser" den von Ihnen konfigurierten Koordinationsrechner aus, und klicken Sie auf "Entsperren".

Verwalten des Koordinationsrechner-Hosts

Wenn Sie einen Koordinationsrechner unter dem Knoten "Koordinationsrechner" auswählen, sind die angezeigten Details anstatt der Kontaktpunkt für den Host relevant.



Weitere Informationen finden Sie unter folgenden Themen, die den Menüoptionen für den Koordinationsrechner-Host zugeordnet sind.

- Quarantäne aufheben

  Weitere Informationen finden Sie unter Aufheben der Quarantäne für einen Koordinationsrechner (siehe Seite 205).

- Quarantäne

  Weitere Informationen finden Sie unter Festlegen der Quarantäne für einen Koordinationsrechner (siehe Seite 204).

- Kontaktpunkt konfigurieren in

  Weitere Informationen finden Sie unter Eigenschaften eines Koordinationsrechner-Kontaktpunkts (siehe Seite 186).

- Entsperren: Wählen Sie den Koordinationsrechner aus, und klicken Sie auf "Entsperren".
- Sperren: Wählen Sie den Koordinationsrechner aus, und klicken Sie auf "Sperren".
- Umbenennen: Wählen Sie den Koordinationsrechner aus, und geben Sie einen neuen Namen ein.
- Löschen:Wählen Sie den Koordinationsrechner aus, und klicken Sie auf "Löschen". Sie können den Domänen-Koordinationsrechner nicht löschen.
- Aktualisieren: Wählen Sie den Koordinationsrechner aus, und klicken Sie auf "Aktualisieren".

Festlegen der Quarantäne für einen Koordinationsrechner

Sie können einen Koordinationsrechner mit Ausnahme des Domänen-Koordinationsrechners unter Quarantäne stellen. Unter Quarantäne wird ein Koordinationsrechner isoliert. Operatoren können auf einem unter Quarantäne gestellten Koordinationsrechner nicht ausgeführt werden. Sie können die Bibliothek eines unter Quarantäne gestellten Koordinationsrechners nicht öffnen. Deswegen können Sie Bibliotheksobjekte auf einem unter Quarantäne gestellten Koordinationsrechner nicht erstellen oder speichern.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Klicken Sie mit der rechten Maustaste auf die Domäne, und wählen Sie "Sperren" aus.
3. Klicken Sie mit der rechten Maustaste auf die Umgebung, die den Koordinationsrechner enthält, den Sie unter Quarantäne stellen möchten, und wählen Sie "Sperren" aus.

4. Erweitern Sie den Knoten "Koordinationsrechner".
5. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, den Sie unter Quarantäne stellen möchten, und wählen Sie "Sperren" aus.
6. Klicken Sie erneut mit der rechten Maustaste auf den Koordinationsrechner, und wählen Sie "Quarantäne" aus.
7. Klicken Sie auf "Speichern".
8. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, und wählen Sie "Entsperren" aus.
9. Klicken Sie mit der rechten Maustaste auf die gesperrte Umgebung, und wählen Sie "Entsperren" aus.
10. Klicken Sie mit der rechten Maustaste auf die Domäne, und wählen Sie "Entsperren" aus.

Aufheben der Quarantäne für einen Koordinationsrechner

Wenn die Quarantäne aus anderen Gründen als das Entfernen des Koordinationsrechners erstellt wurde, dann entfernen Sie die Quarantäne aus dem Koordinationsrechner, wenn die Quarantäne nicht mehr benötigt wird.

So heben Sie die Quarantäne für einen Koordinationsrechner auf:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie das Auswahlmenü "Koordinationsrechner".
3. Klicken Sie mit der rechten Maustaste auf Ziel mit dem unter Quarantäne gestellten Koordinationsrechner, und klicken Sie dann auf "Sperren".
4. Klicken Sie erneut mit der rechten Maustaste auf den Koordinationsrechner, und klicken Sie auf "Quarantäne aufheben".
5. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, und wählen Sie "Entsperren" aus.

   Das Dialogfeld "Nicht gespeicherte Daten" wird geöffnet, in dem Sie danach gefragt werden, ob Sie die Änderungen speichern möchten.
6. Klicken Sie auf "Ja".

Anhalten des Koordinationsrechners

Nur Administratoren mit Administratoren-Anmeldeinformationen auf dem Server, auf dem der Koordinationsrechner installiert ist, können den Koordinationsrechner anhalten.

Wichtig! Wenn ein Koordinationsrechner nicht ordnungsgemäß heruntergefahren wird, können sich im folgenden temporären Ordner Dateien mit einem Volumen von mehreren GB anhäufen. Wenn dies geschieht, können Sie den folgenden temporären Ordner ohne Bedenken löschen:

Installationsverzeichnis/server/c2o/tmp

Gehen Sie folgendermaßen vor:

1. Melden Sie sich mit Administratoren-Anmeldeinformationen am Host an, auf dem der Ziel-Koordinationsrechner installiert ist.
2. Wenn Sie bei einem Windows-Host angemeldet sind, können Sie den Koordinationsrechner-Service vom Startmenü, über das Fenster "Dienste" oder von der Befehlszeile aus anhalten. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie im Startmenü die Option "Programme", "CA", "CA Process Automation 4.0" und "Koordinationsrechner-Service anhalten" aus.
   - Wählen Sie in der Systemsteuerung die Option "Verwaltung" und dann "Dienste". Wählen Sie die folgenden Service aus, und klicken Sie auf "Ende".

     ```
     CA Process Automation-Koordinationsrechner
     (C:\Programme\CA\PAM\server\c2o)
     ```
   - Öffnen Sie eine Eingabeaufforderung, und führen Sie das folgende Skript aus:

     Installationsverzeichnis/server/c2o/bin/stopc2osvc.bat
3. Wenn Sie auf einem UNIX- oder Linux-Host angemeldet sind, führen Sie folgende Schritte aus:
   a. Wechseln Sie die Verzeichnisse zu "${PAM_HOME}/server/c2o/". Ändern Sie zum Beispiel Verzeichnisse zu:

      ```
      /usr/local/CA/PAM/server/c2o
      ```
   b. Führen Sie das Skript "c2osvrd.sh" mit der Option "stop" aus. Zum Beispiel:

      ```
      ./c2osvrd.sh stop
      ```

Starten des Koordinationsrechners

Nur Administratoren mit Administratoren-Anmeldeinformationen auf dem Server, auf dem der Koordinationsrechner installiert ist, können den Koordinationsrechner-Service neu starten.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich mit Administratoren-Anmeldeinformationen am Host an, auf dem der Ziel-Koordinationsrechner installiert ist.

2. Wenn Sie bei einem Windows-Host angemeldet sind, können Sie den Koordinationsrechner-Service vom Startmenü, über das Fenster "Dienste" oder von der Befehlszeile aus neu starten. Führen Sie eine der folgenden Aufgaben aus:

   - Wählen Sie im Startmenü die Option "Programme", "CA", "CA Process Automation" und "Koordinationsrechner-Service starten" aus.

   - Wählen Sie in der Systemsteuerung die Option "Verwaltung" und dann "Dienste". Wählen Sie den folgenden Service aus, und klicken Sie auf "Start".

     ```
     CA Process Automation-Koordinationsrechner
     (C:\Programme\CA\PAM\server\c2o)
     ```

   - Öffnen Sie eine Eingabeaufforderung, und führen Sie das folgende Skript aus:

     Installationsverzeichnis/server/c2o/bin/startc2osvc.bat

3. Wenn Sie auf einem UNIX- oder Linux-Host angemeldet sind, führen Sie folgende Aufgaben aus:

   a. Wechseln Sie die Verzeichnisse zu "${PAM_HOME}/server/c2o/". Ändern Sie zum Beispiel Verzeichnisse zu:

      ```
      /usr/local/CA/PAM/server/c2o
      ```

   b. Führen Sie das Skript "c2osvrd.sh" mit der Option "start" aus. Führen Sie daher Folgendes aus:

      ```
      ./c2osvrd.sh start
      ```

Hinweis: Nachdem Sie den Service für den Domänen-Koordinationsrechner gestartet haben, starten Sie CA Process Automation.

Bereinigen von archivierten Prozessinstanzen von einem Koordinationsrechner

Sie können die Prozessinstanzen bedarfsgesteuert bereinigen, die während eines von Ihnen angegebenen Datumsbereichs ausgeführt wurden.

Bereinigen Sie in den folgenden Situationen archivierte Prozessinstanzen der Laufzeitdatenbank eines Koordinationsrechners:

- Sie benötigen mehr verfügbaren Speicherplatz: Die Kumulierung der archivierten Instanzen beeinträchtigt die Leistung.
- Sie legen die Richtlinie des Koordinationsrechners so fest, dass die automatische Bereinigung ausgeschaltet wird.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie den Knoten "Koordinationsrechner" im Konfigurationsbrowser.

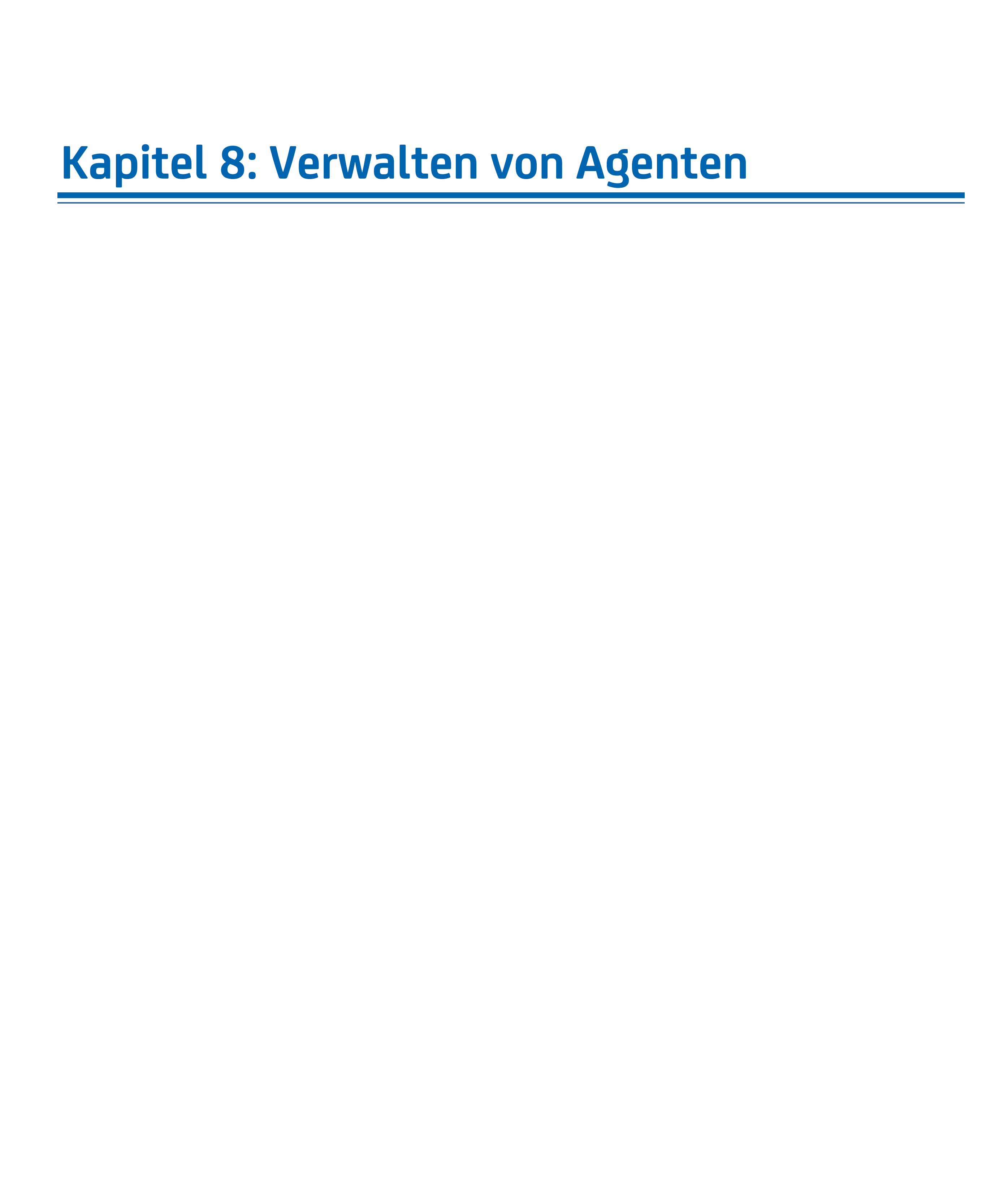
   Der erweiterte Knoten zeigt alle Koordinationsrechner in der Domäne an.

2. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, der die archivierten Prozessinstanzen enthält, die bereinigt werden sollen, und klicken Sie dann auf "Sperren".
3. Klicken Sie auf die Registerkarte "Richtlinien".
4. Klicken Sie im unteren Bereich auf die Schaltfläche "Archivierte Instanz löschen".
5. Definieren Sie im Dialogfeld "Archivierte Instanz löschen" den Datumsbereich, in dem archivierte Instanzen bereinigt werden sollen.
   a. Klicken Sie auf die Kalenderschaltfläche "Anfangsdatum", und wählen Sie "Heute" oder ein Startdatum aus, das vor dem heutigen Datum liegt.
   b. Klicken Sie auf die Kalenderschaltfläche "Enddatum", und wählen Sie "Heute" oder ein Enddatum aus, das nach dem heutigen Datum liegt.
   c. Klicken Sie auf OK.
6. Klicken Sie in der Bestätigungsmeldung auf Ja.

   Der Bereinigungsprozess löscht alle archivierten Instanzen, die innerhalb des angegebenen Datumsbereichs ausgeführt werden.

7. Klicken Sie mit der rechten Maustaste auf den Koordinationsrechner, und klicken Sie dann auf "Entsperren".

Kapitel 8: Verwalten von Agenten



Ein Agent ist eine Komponente, die Sie auf mehreren Hosts in jeder Umgebung installieren. Nachdem Sie einen Agenten auf einem Host installiert haben, konfigurieren Sie einen Kontaktpunkt (eine logische Entität), der die aktuelle Umgebung mit dem Agentenhost verknüpft.

Agenten unterstützen die Ausführung von Prozessen. Prozesse bestehen aus Operatoren. Die meisten Operatoren werden auf dem Koordinationsrechner ausgeführt. Wenn ein Operator auf einem Agentenhost ausgeführt wird, geschieht dies unter Anweisung des Koordinationsrechners, und die Ergebnisse werden an den Koordinationsrechner zurückgegeben. Der Koordinationsrechner führt den Hauptprozess aus.

Um sicherzustellen, dass ein Agentenhost immer für die Verarbeitung verfügbar ist, ordnen Sie einem einzelnen Kontaktpunkt mehrere Agentenhosts zu. Ein Kontaktpunkt ordnet einer angegebenen Umgebung einen oder mehr Agenten zu. Inhaltsdesigner zielen normalerweise auf einen Agentenhost ab, indem sein Kontaktpunkt als Ziel festgelegt wird.

Um Operatoren auf Remote-Hosts auszuführen, die keinen Agenten haben, ordnen Sie Proxy-Kontaktpunkten oder Hostgruppen einen Agenten zu. Operationen können auf einem Remote-Host ausgeführt werden, der über keinen Agenten verfügt, wenn eine SSH-Verbindung vom Agentenhost zum Ziel-Remote-Host konfiguriert ist. Für eine Ausführung auf einem Remote-Host zielen Operatoren auf den Proxy-Kontaktpunkt ab.

Informationen zum Konfigurieren eines Failovers oder Lastenausgleichs unter Agenten, die dem gleichen Kontaktpunkt zugewiesen sind, finden Sie unter Verwalten von Kontaktpunkten (siehe Seite 235).

Informationen zum Einrichten von SSH-Verbindungen finden Sie unter Verwalten von Proxy-Kontaktpunkten (siehe Seite 257) und Verwalten von Hostgruppen (siehe Seite 265).

Dieses Kapitel enthält folgende Themen:

Konfigurieren von Agenten zur Unterstützung von Operatorzielen

Die Agentenkonfiguration in einer Designumgebung ist normalerweise darauf beschränkt, ein kleines Set von Kontaktpunkten zu konfigurieren, von denen jeder einem einzelnen Agent zugeordnet ist. Wenn Hosts knapp sind, können Sie mehrere Kontaktpunkte dem gleichen Agenten zuordnen.

Robustere Agentenkonfigurationen finden sich normalerweise in Produktionsumgebungen. Sechs Optionen werden zunächst einzeln präsentiert und dann zu Referenzzwecken als Überblick in einer Tabelle. Verwenden Sie diese Details, um die Agentenkonfiguration in der Produktionsumgebung zu planen und zu implementieren.

Der Operator wird auf einem bestimmten Agentenhost ausgeführt.

Diese Option ist am einfachsten umzusetzen, wenn ein Operator auf einem Host mit einem Agenten ausgeführt wird. Diese Option ist in einer Entwicklungs- oder Testumgebung zulässig.

Tatsächliches Ziel

Hostname oder IP-Adresse des Zieles.

Installationsanforderung

Installieren Sie einen Agenten auf dem Zielhost.

Zuordnungsanforderung

Definieren Sie einen Kontaktpunkt, der einen Agenten einer Produktionsumgebung zuordnet.

Operatorziel

Geben Sie den Kontaktpunktnamen ein. Alternativ können Sie die Agent-ID eingeben.

Operator wird auf dem Agenten mit der höchsten Priorität unter mehreren möglichen Agenten ausgeführt.

Mit dieser Option können Sie angeben, dass der Operator auf dem besten Host ausgeführt wird, sofern verfügbar, und anderenfalls auf dem nächsten besten. Sie entscheiden, wann ein Host besser ist als ein anderer. Sie können einen Kontaktpunkt konfigurieren, sodass ein bestimmter Operator immer auf dem Host mit der größten Kapazität ausgeführt wird. Alternativ können Sie solche Hosts reservieren und die Ausführung nur dann auf diesen durchführen, wenn alle anderen Kandidaten beschäftigt sind.

Tatsächliches Ziel

Unbekannt. Zeichnen Sie die Hostnamen der Kandidatenzielhosts in der gewünschten Reihenfolge auf.

Installationsanforderung

Installieren Sie einen Agenten auf jedem Kandidatenzielhost.

Zuordnungsanforderung

Definieren Sie einen Kontaktpunkt, und ordnen Sie ihn jedem Kandidatenzielhost zu. Geben Sie in der Kontaktpunktdefinition die Priorität für jeden an.

Operatorziel

Geben Sie den Kontaktpunktnamen ein.

Operator wird auf dem Agenten mit der geringsten Auslastung unter mehreren möglichen Agenten ausgeführt.

Die Implementierung dieser Option dauert länger als die eines Kontaktpunkts, der einem Agenten zugeordnet ist, aber es ist eine stabile Option, wenn auf einen Host mit einem Agenten verwiesen wird. Diese Option wurde für eine Produktionsumgebung entworfen, in der es wichtig ist, dass die Prozesse zum geplanten Zeitpunkt ausgeführt werden.

Tatsächliches Ziel

Unbekannt. Zeichnen Sie die Hostnamen der Kandidatenzielhosts auf.

Installationsanforderung

Installieren Sie einen Agenten auf jedem Kandidatenzielhost.

Zuordnungsanforderung

Definieren Sie einen Kontaktpunkt, und ordnen Sie ihn jedem Kandidatenzielhost zu. Geben Sie in der Kontaktpunktdefinition die gleiche Zahl wie die Priorität für jede Zuordnung ein. Diese Implementierung dient dem Lastenausgleich.

Operatorziel

Geben Sie den Kontaktpunktnamen ein.

Operator wird auf mehreren Agentenhosts gleichzeitig ausgeführt.

Wenn Sie die Kontaktpunktgruppe verwenden, können Sie einen Operator gleichzeitig auf allen den Kontaktpunkten in der Gruppe zugeordneten Hosts ausführen.

Tatsächliche Ziele

Zeichnen Sie den Hostnamen für jeden Zielhost auf.

Installationsanforderung

Installieren Sie einen Agenten auf jedem Zielhost.

Zuordnungsanforderung

- Definieren Sie einen eigenen Kontaktpunkt für jeden dieser Agenten.
- Definieren Sie eine aus diesen Kontaktpunkten bestehende Kontaktpunktgruppe.

Operatorziel

Geben Sie den Kontaktpunktgruppennamen ein.

Operator wird auf einem bestimmten Remote-Host ausgeführt.

Manchmal können Sie einen Agenten nicht auf dem Host installieren, den Sie für den Operator als Ziel verwenden wollen. Definieren Sie in diesem Fall einen Agenten als Proxy-Kontaktpunkt. Erstellen Sie eine SSH-Verbindung von dem Host mit dem Agenten zu dem Ziel-Remote-Host.

Tatsächliches Ziel

Zeichnen Sie den Hostnamen oder die IP-Adresse des Remote-Hosts auf, der das Ziel ist.

Quellhost aktivieren

Zeichnen Sie den Hostnamen des Quellhosts auf, der über eine SSH-Verbindung mit dem Ziel verbunden werden kann.

Konnektivitätsanforderung

Erstellen Sie die SSH-Verbindung vom Quellhost zum Remote-Host.

Installationsanforderung

Installieren Sie einen Agenten auf dem Quellhost.

Zuordnungsanforderung

Definieren Sie einen Proxy-Kontaktpunkt auf dem Quellhost, und geben Sie Details zur Verbindung mit dem Remote-Zielhost an.

Operatorziel

Geben Sie den Proxy-Kontaktpunkt-Namen ein.

Operator wird auf einem Remote-Host ausgeführt, auf dem sich das Ziel bei jeder Ausführung ändern kann.

Mit dieser Option können Sie direkt vor der Laufzeit entscheiden, auf welchen Remote-Host Sie verweisen möchten, wenn Sie das Ziel mit dem Hostnamen oder der IP-Adresse angeben. Das Ziel muss Mitglied einer Hostgruppe sein. Eine Hostgruppe ist eine Gruppe, die entweder ein gemeinsames Hostnamenmuster oder ein gemeinsames IP-Adressen-Muster aufweist. Hosts mit einem gemeinsamen IP-Adressenmuster gehören zum gleichen Subnetz.

Tatsächliches Ziel

Unbekannt. Zeichnen Sie die Hostnamen der remoten Kandidatenziel-Hosts auf.

Quellhost aktivieren

Zeichnen Sie den Hostnamen des Quellhosts auf, der über eine SSH-Verbindung mit jedem Kandidatenziel verbunden werden kann.

Konnektivitätsanforderung

Erstellen Sie die SSH-Verbindung vom Quellhost zu jedem Remote-Host.

Installationsanforderung

Installieren Sie einen Agenten auf dem Quellhost.

Zuordnungsanforderung

Definieren Sie eine Hostgruppe auf dem Quellhost mit einem Muster, das von allen Remote-Hosts genutzt wird.

Operatorziel

Geben Sie den Hostnamen oder die IP-Adresse des Remote-Zielhosts ein. Drücken Sie das Operatorziel in einem Datensatz aus. Sie können Datensätze selbst dann ändern, wenn sie durch einen nicht änderbaren Prozess importiert wurden.

Verwenden Sie die folgende Tabelle als Richtlinie für das Erstellen von Überblicktabellen. Eine Dokumentation in Form von Überblicktabellen kann anderen dabei helfen, diese Informationen zu finden, wenn Sie gerade einmal nicht verfügbar sind.

Zieltyp	Agent-Zuordnung	Sonstige Konfiguration	Operatorziel
Ein einzelner Host	Ein neuer Kontaktpunkt	N. rel.	Kontaktpunktname
Einer von mehreren Hosts, nach Priorität sortiert	Ein vorhandener Kontaktpunkt	Geben Sie die Priorität an, mit der der Zielhost ausgewählt wird.	Kontaktpunktname
Einer von mehreren Hosts (ohne Priorität)	Ein vorhandener Kontaktpunkt	Weisen Sie jedem Kandidaten-Zielhost die gleiche Priorität zu.	Kontaktpunktname

Zieltyp	Agent-Zuordnung	Sonstige Konfiguration	Operatorziel
Mehrere Hosts gleichzeitig	Ein neuer Kontaktpunkt	Erstellen Sie eine Kontaktpunktgruppe mit allen Kontaktpunkten.	Kontaktpunktgruppen name
Einzelner Remote-Host	Ein Proxy-Kontaktpunkt	Erstellen Sie eine SSH-Verbindung vom Agentenhost zum Remote-Zielhost.	Proxy-Kontaktpunktna me
Einer von mehreren Remote-Hosts	Eine Hostgruppe	Erstellen Sie eine SSH-Verbindung vom Agentenhost zu jedem Remote-Zielhost.	Zielhostname oder IP-Adresse

Weitere Informationen

Informationen zur Agent-Kommunikation (siehe Seite 232)

Interaktives Installieren eines Agenten

Prozesse können Operatoren enthalten, die auf Servern mit einer Zielanwendung, einer Datenbank oder einem System ausgeführt werden müssen. Installieren Sie nach Möglichkeit einen Agenten auf solch einem Server. Wenn dies nicht möglich ist, installieren Sie den Agenten auf einem Host, der mit diesem Server über SSH eine Verbindung herstellen kann.

Wichtig! Bevor Sie einen Agenten installieren, stellen Sie sicher, dass der Domänen-Koordinationsrechner ausgeführt wird.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie auf das Auswahlmenü "Installation".
3. Klicken Sie auf "Installieren" für "Agent installieren".

   Es wird ein Dialogfeld angezeigt, das den Fortschritt für das Herunterladen der Anwendung veranschaulicht.
4. Wenn Sie eine Sicherheitswarnung erhalten, klicken Sie auf "Ausführen".

   Das Dialogfeld "Sprachauswahl" wird geöffnet. Die Sprache des Hostcomputers wird standardmäßig ausgewählt.

5. Klicken Sie auf "OK" oder wählen Sie eine andere Sprache aus, und klicken Sie auf "OK".

   Die "Willkommen"-Seite des Setup-Assistenten für den CA Process Automation-Agent wird angezeigt.

6. Klicken Sie auf "Weiter".

   Die Lizenzvereinbarung wird geöffnet.

7. Lesen Sie die Lizenzvereinbarung. Wenn Sie die Bedingungen akzeptieren, klicken Sie auf "Ich akzeptiere die Bedingungen der Lizenzvereinbarung". Klicken Sie auf "Weiter".

   Die Seite "Legen Sie das Java-Home-Verzeichnis fest" wird geöffnet.

8. Wenn das angezeigte Java-Home-Verzeichnis nicht richtig ist, navigieren Sie zum JRE-Ordner.

   Alle Plattformen unterstützen "jre6", Windows unterstützt "jre6" und "jre7".

   Nachfolgend wird ein Beispielpfad für die Windows-Plattform angegeben:

   ```
   C:\Programme\Java\jdk1.7.0_45
   ```

9. Klicken Sie auf "Weiter".

   Die Seite zum Auswählen des Zielverzeichnisses wird geöffnet. Auf Windows-Hosts folgt der Standardpfad:

   ```
   C:\Programme\CA\PAM Agent
   ```

10. Klicken Sie auf "Weiter", um das Standardverzeichnis zu akzeptieren oder geben Sie ein Zielverzeichnis für den neuen Agenten ein, und klicken Sie auf "Weiter".

    Die Seite zum Auswählen des Startmenüordners wird geöffnet.

11. (Nur für Windows) Klicken Sie auf "Weiter", um den CA Process Automation-Agent als Ihre Startmenü-Verknüpfung zu akzeptieren oder geben Sie einen neuen Namen ein, und klicken Sie auf "Weiter".

    - (Optional) Erstellen Sie Verknüpfungen für alle Anwender auf diesem Host.
    - (Optional) Erstellen Sie keinen Startmenüordner.

12. Überprüfen Sie die URL der Domäne. Dabei handelt es sich um die URL, über die Sie die Agenteninstallation gestartet haben. Klicken Sie auf "Weiter".

13. Wenn die Domäne gesichert ist, geben Sie ein Kennwort an.
14. Stellen Sie die Seite "Allgemeine Eigenschaften" fertig, und klicken Sie dann auf "Weiter".
    a. Geben Sie in Agenten-Host den Namen des Agenten-Host ein. Dieser Name identifiziert den Host, von dem Sie die Installation gestartet haben.
    b. Ändern Sie oder akzeptieren Sie den standardmäßigen Anzeigenamen, den Hostnamen.
    c. Wenn Sie die Agenteninstallation von einem Windows-Host gestartet haben, wählen Sie "Als Windows-Dienst installieren" aus.
    d. Um eine neue Verbindung für jede Kommunikation von einem Koordinationsrechner zu einem Agenten zu erzwingen, wählen Sie "Veraltete Kommunikation verwenden" aus.

       Wir empfehlen, dass Sie dieses Kontrollkästchen *deaktivieren*. Vereinfachte Kommunikationen, die Standardeinstellung, wird bevorzugt, weil eine persistente Verbindung verwendet wird.
    e. Wenn Sie "Veraltete Kommunikation verwenden" ausgewählt haben, akzeptieren Sie 7003 als Agentenport, sofern dieser Port nicht verwendet wird. Wenn der Standardport verwendet wird, geben Sie eine nicht verwendete Portnummer wie z. B. 57003 als Port ein, auf dem der Agent die Kommunikation mit Koordinationsrechnern überwacht.

       Hinweis: Wenn die veraltete Kommunikation nicht verwendet wird, dann verwenden Koordinationsrechner eine Web-Socket-Verbindung (von Agenten eingerichtet), um mit Agenten zu kommunizieren. Koordinationsrechner verwenden Port 80, um mit Agenten über HTTP zu kommunizieren. Koordinationsrechner verwenden Port 443, um mit Agenten über HTTPS zu kommunizieren.
    f. Wählen Sie Agenten-Service nach Installation starten aus.

       Das Starten des Agenten ermöglicht es Ihnen, den aktiven Agenten anzuzeigen und mit der Agentenkonfiguration fortzufahren.
15. Klicken Sie auf "Weiter", um das standardmäßige temporäre Verzeichnis für die Ausführung von Skripten zu akzeptieren, oder geben Sie einen anderen Pfad ein, und klicken Sie anschließend auf "Weiter".

    Hinweis: Ein gültiger Pfad enthält keine Leerzeichen.

    Die Seite "PowerShell-Ausführungsrichtlinie festlegen" wird angezeigt.

16. Stellen Sie die Einstellung mit einer der folgenden Methoden fertig.
    - Um Windows PowerShell-Skripte über diesen Agenten auszuführen:
        a. Aktivieren Sie das Kontrollkästchen "PowerShell-Ausführungsrichtlinie festlegen".
        b. Navigieren Sie zum Speicherort des PowerShell-Hosts, wenn dieser vom angezeigten Standard abweicht.
        c. Klicken Sie auf "Weiter".
    - Wenn Sie Windows PowerShell nicht verwenden, klicken Sie auf "Weiter".

    Die Agenteninstallation wird gestartet.
17. Klicken Sie auf "Fertig stellen".
18. (Nur für Windows) Starten Sie den Agenten-Service. Klicken Sie auf "Start", "Programme", "CA", "CA Process Automation-Agent", "Agenten-Service starten".
19. Klicken Sie im Auswahlmenü "Konfigurationsbrowser" auf der Registerkarte "Konfiguration".
20. Klicken Sie auf "Aktualisieren". (Oder: melden Sie sich ab, und melden Sie sich wieder an.)
21. Erweitern Sie "Agenten", und stellen Sie sicher, dass Ihr Agentenname aufgelistet ist.

    Hinweis: Um den Agenten-Host als Ziel zu verwenden, konfigurieren Sie einen Kontaktpunkt. Um den Agenten-Host als Gateway zu einem Remote-Host zu verwenden, konfigurieren Sie einen Proxy-Kontaktpunkt.

Fügen Sie einen Agentenkontaktpunkt hinzu.

Wenn Sie einen Agenten auf einem Host installieren, wird der Anzeigename des Agent unter dem Knoten "Agenten" angezeigt. Damit ein Operator diesen Host als Ziel festlegen kann, konfigurieren Sie einen Kontaktpunkt, der auf den Host verweist.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie den Knoten "Agenten".
3. Klicken Sie mit der rechten Maustaste auf den Agenten, wählen Sie "Kontaktpunkt konfigurieren in" aus, und wählen Sie anschließend die *Umgebung* aus.

    Es wird eine Aufforderung zum Sperren der ausgewählten Umgebung angezeigt.
4. Klicken Sie auf "Ja", um die ausgewählte Umgebung zu sperren.

    Das Dialogfeld Agentenkontaktpunkt hinzufügen wird angezeigt.

5. Geben Sie für den neuen Kontaktpunkt einen Namen ein, der sich vom Hostnamen unterscheidet, und klicken Sie auf "OK".

   Der neue Kontaktpunkt wird für die zugeordnete Umgebung unter dem Knoten "Alle Kontaktpunkte" angezeigt.

6. Klicken Sie auf "Speichern".

7. Klicken Sie auf die gesperrte Umgebung, und klicken Sie auf "Entsperren".

Hinzufügen einer Agentenhostgruppe

Wenn ein Operator direkt auf Remote-Hosts abzielen muss (mit einer IP-Adresse oder einem Hostnamen), können Sie folgende Aktionen durchführen:

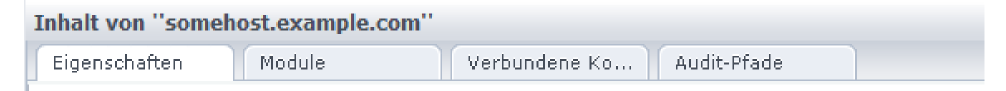
1. Erstellen einer Hostgruppe (siehe Seite 269).
2. Konfigurieren der Eigenschaften einer Hostgruppe (siehe Seite 270). Sie können bestimmte Remote-Hosts hinzufügen, oder Sie können Muster eingeben, die Hosts enthalten, die Sie als Ziel festlegen möchten.
3. Erstellen von SSH-Anmeldeinformationen auf Hosts in einer Hostgruppe (siehe Seite 274). Das bedeutet: Erstellen Sie ein Anwenderkonto auf allen Remote-Hosts mit den Anmeldeinformationen, die bei den Eigenschaften der Hostgruppe eingegeben wurden.

Weitere Informationen:

Verwalten von Hostgruppen (siehe Seite 265)

Konfigurieren der Inhalte eines ausgewählten Agenten

Viele Eigenschaftseinstellungen werden während der Agenteninstallation abgerufen. Verbundene Kontaktpunkte sind Konfigurationsdetails, die ausschließlich für Agenten sind und nicht vererbt werden. Einstellungen für Operatoreinstellungen auf der Registerkarte "Module" werden standardmäßig übernommen. Die Einstellungen, die Sie für einen Agenten konfigurieren, unterscheiden sich von den Einstellungen, die Sie für den Agentenkontaktpunkt konfigurieren.



Das Menü "Agent" weist die folgenden Registerkarten auf:

Eigenschaften

Weitere Informationen finden Sie unter Konfigurieren von Agenteneigenschaften (siehe Seite 220).

Module

Weitere Informationen finden Sie unter Anpassen von Agenteneinstellungen für Operatorkategorien. (siehe Seite 221)

Verbundene Kontaktpunkte und Hostgruppen

Weitere Informationen finden Sie unter Anzeigen der Kontaktpunkte und Hostgruppen für einen ausgewählten Agenten (siehe Seite 223).

Audit-Pfade

Weitere Informationen finden Sie unter Anzeigen des Audit-Pfads für einen Agenten (siehe Seite 363).

Konfigurieren von Agenteneigenschaften

Sie können Werte für folgende Agenteneigenschaften festlegen:

- Sie können angeben, wie oft der Agent ein Heartbeat-Signal zum Domänen-Koordinationsrechner senden soll.
- Sie können angeben, wie oft der Agent den Domänen-Koordinationsrechner nach Aktualisierungen prüft.

Der Agent sendet ein Heartbeat-Signal beim Start und beim konfigurierten Ablaufplan, während der Agent aktiv ist. Der Domänen-Koordinationsrechner bestätigt das Heartbeat-Signal oder die Domänenaktualisierungen, sofern vorhanden. Der Domänen-Koordinationsrechner sendet dem Agenten gemäß den festgelegten Spiegelungsintervallen gespiegelte Aktualisierungen.

Sie können Agenteneigenschaften im Konfigurationsbrowser festlegen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie die Option "Agenten" im Auswahlmenü "Konfigurationsbrowser".
2. Wählen Sie den Agenten aus, den Sie konfigurieren möchten, und klicken Sie auf "Sperren".
3. Wählen Sie die Registerkarte "Eigenschaften" für den ausgewählten Agenten aus.

4. (Optional) Überprüfen Sie folgende schreibgeschützte Eigenschaften:
   - Status - Aktiv oder Inaktiv
   - Agentenname - Name, der bei der Installation als Anzeigename konfiguriert wurde.
   - Hostname - Name, der bei der Installation als Agenten-Host konfiguriert wurde.
   - Hostadresse
5. (Optional) Aktualisieren Sie folgende Eigenschaften:
   - Spiegelungsintervall (Minuten)
   - Heartbeat-Intervall (Minuten) - Standardwert auf der Domänenebene ist 2.
   - Veraltete Kommunikation verwenden
6. Wählen Sie den Agenten aus, und klicken Sie auf "Entsperren".
7. Klicken im Dialogfeld "Ungespeicherten Daten" auf "Ja", um die Änderungen zu speichern.

Anpassen der Operatorkategorien für einen ausgewählten Agenten

Alle Umgebungen, Koordinationsrechner und Agenten übernehmen Einstellungen, die Sie auf der Registerkarte "Module" für die Domäne konfiguriert haben. Administratoren können die Konfiguration an niedrigeren Ebenen der Domänen-Hierarchie bearbeiten. Administratoren können Operatorkategorien auf sämtlichen Agenten aktivieren und die Konfigurationen nach Bedarf ändern.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Blenden Sie Agenten ein, klicken Sie mit der rechten Maustaste auf den anzupassenden Agenten, wählen Sie "Sperren" aus.
3. Klicken Sie auf die Registerkarte "Module".
4. Wählen Sie aus der Drop-down-Liste "Aktivieren/Deaktivieren" die Option "Aktiviert" für die zu bearbeitende Operator-Kategorie aus.
5. Klicken Sie mit der rechten Maustaste auf die gleiche Kategorie, und wählen Sie "Bearbeiten" aus.

6. Ändern Sie die Eigenschaftseinstellungen der ausgewählte Kategorie für den ausgewählten Agenten. Weitere Informationen finden Sie in den folgenden Beschreibungen von Feldern auf Domänenebene:
   - Konfigurieren von Catalyst (siehe Seite 291).
   - Konfigurieren der Befehlsausführung. (siehe Seite 297)
   - Konfigurieren von Datenbanken: Oracle-Eigenschaften (siehe Seite 304).
   - Konfigurieren von Datenbanken: MS SQL Server-Eigenschaften (siehe Seite 306).
   - Konfigurieren von Datenbanken: MySQL-Eigenschaften (siehe Seite 308).
   - Konfigurieren von Datenbanken: Sybase-Eigenschaften (siehe Seite 309).
   - Konfigurieren von Directory-Service (siehe Seite 311).
   - Konfigurieren von E-Mail (siehe Seite 313).
   - Konfigurieren der Dateiverwaltung (siehe Seite 315).
   - Konfigurieren des Dateigtransfers. (siehe Seite 317)
   - Konfigurieren von Netzwerk-Hilfsprogrammen (siehe Seite 319).
   - Konfigurieren der Prozesssteuerung (siehe Seite 321).
   - Konfigurieren von Hilfsprogrammen (siehe Seite 322).
   - Konfigurieren von Webservices (siehe Seite 323).
7. Klicken Sie auf "Speichern", und klicken Sie in der Verifizierungsmeldung auf "OK".
8. Klicken Sie mit der rechten Maustaste auf den gesperrten Agenten, und wählen Sie "Entsperren" aus.

Deaktivieren einer Operatorkategorie auf einem ausgewählten Agenten

Auf der Registerkarte "Module" für einen ausgewählten Agenten können Sie eine oder mehrere Operatorkategorien für diesen Agenten deaktivieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie die Option "Agenten" im Auswahlmenü "Konfigurationsbrowser".
2. Wählen Sie den Agenten aus, den Sie konfigurieren möchten, und klicken Sie auf "Sperren".
3. Klicken Sie auf die Registerkarte "Module".
4. Wählen Sie eine Operatorkategorie aus, für die "Aktivieren/Deaktivieren" für "Aktivieren" oder "Von Umgebung übernehmen" festgelegt wird.
5. Wählen Sie in der Drop-down-Liste "Aktivieren/Deaktivieren" die Option "Deaktivieren" aus.

6. Klicken Sie auf "Speichern".
7. Klicken Sie auf Entsperren.

   Das Produkt deaktiviert die ausgewählte Operatorkategorie auf dem ausgewählten Agenten.

Konfigurieren eines ausgewählten Kontaktpunkts oder einer Hostgruppe

Ein Kontaktpunkt ist eine Zuordnung zwischen einem Agenten (oder Koordinationsrechner) und einer Umgebung. Ein Proxy-Kontaktpunkt ist eine Zuordnung zwischen einem Agenten, einem Remote-Host und einer Umgebung. Eine Hostgruppe ist eine Zuordnung zwischen einem Agenten, einer Gruppe von Remote-Hosts und einer Umgebung.

Wenn Sie einem Agenten einen Kontaktpunkt oder Proxy-Kontaktpunkt hinzufügen, wird dieser Kontaktpunkt unter "Alle Kontaktpunkte" angezeigt.

Wenn Sie einem Agenten eine Hostgruppe hinzufügen, wird dieser Hostgruppenname unter "Alle Hostgruppen" angezeigt.

Weitere Informationen zu den Konfigurationsdetails finden Sie unter folgenden Themen:

- Verwalten von Kontaktpunkten (siehe Seite 235).
- Verwalten von Proxy-Kontaktpunkten (siehe Seite 257).
- Verwalten von Hostgruppen (siehe Seite 265).

Anzeigen der Kontaktpunkte und Hostgruppen für einen ausgewählten Agenten

Sie können die Kontaktpunkte und Hostgruppen für einen ausgewählten Agenten auf der Registerkarte "Verbundene Kontaktpunkte" anzeigen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie die Option "Agenten" im Auswahlmenü "Konfigurationsbrowser".
2. Wählen Sie den Agenten aus, für den Sie Kontaktpunkte und Hostgruppen anzeigen möchten.
3. Klicken Sie auf die Registerkarte "Verbundene Kontaktpunkte".

   Die Namen der Kontaktpunkte oder Hostgruppen und die Hierarchie (Domäne ist der Stammknoten) werden angezeigt.

Festlegen der Quarantäne für einen Agenten

Unter Quarantäne wird ein Agent von eingehendem oder ausgehendem Netzwerkverkehr von CA Process Automation isoliert. Operatoren können auf einem unter Quarantäne gestellten Agenten nicht ausgeführt werden. Stellen Sie einen Agenten in Quarantäne, wenn Sie nicht möchten, dass der Agent ein CA Process Automation-Operatorziel ist.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie den Knoten "Agenten".
3. Wählen Sie den Agenten aus, den Sie in Quarantäne stellen möchten, und klicken Sie auf "Sperren".
4. Klicken Sie mit der rechten Maustaste auf den Agenten, und wählen Sie "Quarantäne" aus. Der Quarantänemodifikator wird dem Basissymbol des gesperrten Agenten hinzugefügt.

5. Klicken Sie auf "Entsperren".

   Das Dialogfeld "Nicht gespeicherte Daten" wird geöffnet, in dem Sie danach gefragt werden, ob Sie die Änderungen speichern möchten.

6. Klicken Sie auf "Ja".

   Der Quarantänemodifikator wird für den Kontaktpunkt oder für die Hostgruppe angezeigt, der bzw. die dem in Quarantäne gestellten Agenten zugeordnet ist.

Aufheben der Quarantäne für einen Agenten

Sobald der Quarantänezeitraum abgelaufen ist, heben Sie die Quarantäne für den Agenten auf.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie den Knoten "Agenten".
2. Klicken Sie auf den in Quarantäne gestellten Agenten, für den Sie die Quarantäne entfernen möchten, und klicken Sie auf "Sperren".
3. Klicken Sie mit der rechten Maustaste auf den Agenten, und klicken Sie auf "Quarantäne aufheben".
4. Klicken Sie auf "Entsperren".

   Das Dialogfeld "Nicht gespeicherte Daten" wird geöffnet, in dem Sie danach gefragt werden, ob Sie die Änderungen speichern möchten.
5. Klicken Sie auf "Ja".

   Der Sperrmodifikator für das Basissymbol des Agenten wird entfernt. Die Quarantänemodifikatoren für den Agenten und zugeordneten Kontaktpunkt oder die Basissymbole der Hostgruppe werden durch den aktiven Symbolmodifikator ersetzt.

Umbenennen eines Agenten

Der Name für einen Agenten wird während der Agenteninstallation standardmäßig auf den Hostnamen gesetzt. Sie können den Agenten umbenennen. Zum Beispiel könnten Sie den FQDN für den Host durch "Agent-*Hostname*" ersetzen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie die Option "Agenten" im Auswahlmenü "Konfigurationsbrowser".
2. Wählen Sie den Agenten aus, den Sie umbenennen möchten, und klicken Sie auf "Sperren".
3. Klicken Sie mit der rechten Maustaste auf den Agenten, und wählen Sie "Umbenennen" aus.
4. Geben Sie einen neuen Namen ein.
5. Klicken Sie auf "Speichern".
6. Wählen Sie den Agenten aus, und klicken Sie auf "Entsperren".

Identifizieren des Installationspfads eines Agenten

Sie können den Pfad identifizieren, unter dem ein Agent installiert ist. Der Standardpfad für ein Windows 7-Betriebssystem ist:

```
C:\Programme(x86)\CA\Pam Agent\PAMAgent
```

Folgen Sie diesem Schritt:

Verwenden Sie das folgende Skript, um den Agenteninstallationspfad zu identifizieren:

```
echo %C2OHOME%
```

Das Skript gibt den vollständigen Installationspfad des CA Process Automation-Agenten zurück.

Hinweis: Dieses Skript geht davon aus, dass Sie C2OHOME als eine Umgebungsvariable definiert haben.

Verwalten der Stilllegung eines Hosts mit einem Agenten

Wenn Sie benachrichtigt werden, dass Ihr Unternehmen Hardware austauschen möchte, auf der Sie Agenten installiert haben, sollten Sie den folgenden Prozess anwenden, um die Auswirkungen zu minimieren. Dieser Prozess weist die ursprünglichen Kontaktpunkte Agenten zu, die auf neuer Hardware installiert sind. Die Neuzuordnung erlaubt, dass Prozesse, die diese Kontaktpunkte benötigen, ohne Änderungen weiter ausgeführt werden können.

Im Folgenden finden Sie zwei typische Situationen:

- Die alten Hosts werden entfernt, und danach werden die neuen Hosts hinzugefügt. Diese Vorgehensweise ist üblich, wenn IP-Adressen neu zugewiesen werden.
- Der neue Host wird hinzugefügt, und danach wird der alte Host entfernt.

In dem Fall, in dem der Plan darin besteht, alte Hosts vor dem Bereitstellen neuer Hosts zu entfernen, sollten Sie folgendermaßen vorgehen:

1. Gehen Sie folgendermaßen vor, bevor ein Host aus dem Netzwerk entfernt wird:
    a. Identifizieren Sie den Agentennamen in CA Process Automation für den Host, der stillgelegt wird.

        Im Auswahlmenü "Agenten" im Konfigurationsbrowser werden alle Agenten mit ihrem Status aufgelistet.

    b. Identifizieren Sie die Kontaktpunkte, die mit dem zu löschenden Agenten verbunden sind.

        Wählen Sie im Auswahlmenü "Agenten" im Konfigurationsbrowser den Agenten aus, und klicken Sie auf die Registerkarte "Verbundene Kontaktpunkte", um die Liste der Kontaktpunkte anzuzeigen, die für die Neuzuweisung analysiert werden.

    c. Deinstallieren Sie die Agentensoftware von dem Host, der stillgelegt oder anderweitig genutzt wird.
2. Installieren Sie die Agentensoftware auf dem Host, der den stillgelegten Host ersetzt.
3. Verbinden Sie den betroffenen Kontaktpunkt mit dem neuen Agenten.
4. Entfernen Sie den Agenten für den stillgelegten Host aus CA Process Automation.

    Klicken Sie im Auswahlmenü "Agenten" im Konfigurationsbrowser mit der rechten Maustaste auf den Agenten, wählen Sie "Sperren" aus, und klicken Sie dann mit der rechten Maustaste, und wählen Sie "Löschen" aus.

In dem Fall, in dem die neuen Hosts ins Netzwerk gebracht werden, bevor die alten Hosts herausgenommen werden, sollten Sie folgendermaßen vorgehen:

1. Installieren Sie einen Agenten auf jedem neuen Host.
2. Verbinden Sie die betroffenen Kontaktpunkte mit neuen Agenten.
3. Verwenden Sie "Gebündelte Agentenentfernung", um die ersetzten Agenten zu entfernen.

Löschen eines Agenten

Wenn ein Agent, den Sie installiert haben, nicht mehr erwünscht ist, deinstallieren Sie diesen Agenten vom Host. Löschen Sie den Agenten anschließend aus dem Auswahlmenü "Agenten".

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Erweitern Sie die Option "Agenten", und stellen Sie sicher, dass der Zielagent entsperrt ist und sich nicht in Quarantäne befindet.
3. Wählen Sie den Zielagenten aus, und klicken Sie auf "Löschen".

   Ein Dialogfeld zur Bestätigung wird eingeblendet.
4. Klicken Sie auf OK.
5. Klicken Sie auf "Speichern".
6. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Gebündeltes Entfernen ausgewählter Agenten

Wenn für Agenten verwendete Server stillgelegt werden, können Sie die CA Process Automation-Referenzen für diese inaktiven Agenten gebündelt entfernen. Dann können Sie die verbundenen leeren Kontaktpunkte gebündelt entfernen.

Wenn beim Ersetzen der Server jeweils ein Teilnetz ersetzt wird, können Sie die verbundenen Agenten für die Entfernung auswählen, indem Sie eine CIDR-basierte Suche angeben. Wenn die stillgelegten Server in ihren Hostnamen ein gemeinsames Muster aufweisen, können Sie Agenten für die Entfernung basierend auf einem angegebenen Muster auswählen, das den Kriterien entspricht.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie mit der rechten Maustaste auf Domäne, und wählen Sie Sperren aus.
3. Klicken Sie mit der rechten Maustaste auf Domäne, und wählen Sie Gebündelte Agentenentfernung aus.
4. Geben Sie Suchkriterien in eine der folgenden Weisen ein:
   - Wählen Sie Suche nach IP-Adressmuster aus, und geben Sie ein Teilnetz im CIDR-Format ein, das die Ziel-IP-Adressen enthält.
   - Wählen Sie Suche nach Hostnamensmuster aus, und geben Sie einen Suchausdruck ein, der den Domänennamen enthält, zum Beispiel *.*eigenesUnternehmen*.com.
   - Wählen Sie eins der Muster aus, aber lassen Sie das Suchfeldformular leer.
5. Klicken Sie auf Suchen.

   In der Tabelle "Agenten" werden alle Agenten angezeigt, die mit den Suchkriterien übereinstimmen, aber nur inaktive Agenten können zur Entfernung ausgewählt werden.
6. Wählen Sie aus den angezeigten inaktiven Agenten die Agenten aus, die Sie entfernen möchten, und klicken Sie auf Löschen.

   Eine Bestätigungsmeldung, die die Anzahl der ausgewählten Agenten angibt, fragt, ob Sie fortfahren oder abbrechen möchten.
7. Wählen Sie Fortfahren aus.

   Die ausgewählten Agenten werden aus der Domäne entfernt, und die Änderung an der Domäne wird automatisch gespeichert.
8. Klicken Sie mit der rechten Maustaste auf Domäne, und wählen Sie Entsperren aus.

Starten eines Agenten

Verwenden Sie die Methode zum Starten oder erneuten Starten eines Agenten für das Betriebssystem auf dem Host, der den Agenten enthält.

Starten oder erneutes Starten eines Agenten auf einem Microsoft Windows-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem Windows-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows-Host an, auf dem der Agent installiert ist.
2. Wählen Sie im Menü "Start" "Programme", "CA", "CA Process Automation-Agenten", "Agenten-Service starten" aus.
3. Melden Sie sich vom Host ab.

Starten oder erneutes Starten eines Agenten auf einem Linux-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem UNIX- oder Linux-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim UNIX- oder Linux-Host an, auf dem der Agent installiert ist.
2. Nehmen Sie die folgenden Änderungen an Verzeichnissen vor:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Führen Sie folgenden Befehl aus:

   ```
   ./c2oagtd.sh start
   ```

   Der Agent startet neu.

Anhalten von Agenten

Sie können einen CA Process Automation-Agenten anhalten, der auf einem UNIX- oder Linux-Host ausgeführt wird.

Anhalten eines Agenten auf einem Microsoft Windows-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem Windows-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows-Host an, auf dem der Agent installiert ist.
2. Wählen Sie im Menü "Start" "Programme", "CA", "CA Process Automation-Agenten", "Agenten-Service anhalten" aus.
3. Melden Sie sich vom Host ab.

Anhalten eines Agenten auf einem Linux-Host

Die folgenden Schritte gelten für sämtliche Agenten in Ihrer CA Process Automation-Domäne, die sich auf Hosts mit einem UNIX- oder Linux-Betriebssystem befinden.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim UNIX- oder Linux-Host an, auf dem der Agent installiert ist.
2. Nehmen Sie die folgenden Änderungen an Verzeichnissen vor:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Führen Sie folgenden Befehl aus:

   ```
   ./c2oagtd.sh stop
   ```

   Der Agent wird angehalten.

Informationen zur Agent-Kommunikation

Sie konfigurieren Agent-Kommunikationen, wenn Sie einen Agenten installieren. Standardmäßig verwenden neue Agenten vereinfachte Kommunikation (das Kontrollkästchen "Veraltete Kommunikation verwenden" ist deaktiviert).

Agenten, für die ein Upgrade durchgeführt wurde, verwenden veraltete Kommunikation. Sie können diese Einstellung neu konfigurieren, ohne den Agenten neu zu installieren.

Anzeigename WIN-AS1AEUUVCUE.ca.com

Als Windows-Dienst installieren

Veraltete Kommunikation verwenden

Agenten-Service nach Installation starten

Vereinfachte Kommunikation

Die vereinfachte Mitteilung verwendet Web-Sockets und HTTP, um eine einseitige und persistente Verbindung vom Agenten zum Koordinationsrechner herzustellen. CA Process Automation verwendet einen standardmäßigen Port (80 oder 443), der eine schnelle Verbindung zwischen den Komponenten ermöglicht.

Veraltete Kommunikation

Die veraltete Kommunikation mit mehreren Ports kann mit Firewalls und NAT-Routern nicht so gut umgehen wie die vereinfachte Kommunikation. Vom Koordinationsrechner initiierte Verbindungen, die in veralteten Kommunikationsvorgängen verwendet werden, sind weniger effizient als die persistenten Verbindungen, die in vereinfachten Kommunikationsvorgängen verwendet werden.

Konfigurieren von Agenten zur Verwendung von vereinfachter Kommunikation

Sie müssen vorhandene Agenten neu installieren, um von veralteter Kommunikation zu vereinfachter Kommunikation zu wechseln. Dies kann für alle Agenten durchgeführt werden, nachdem Sie ein Upgrade auf CA Process Automation 04.2.00 durchgeführt und einen NGINX-Lastenausgleich installiert und konfiguriert haben.

Informationen zum erneuten Installieren der Agenten finden Sie unter Interaktives Installieren eines Agenten (siehe Seite 215). Standardmäßig ist das Kontrollkästchen "Veraltete Kommunikation verwenden" deaktiviert. Wenn dieses Kontrollkästchen deaktiviert bleibt, werden die Agenten für die Verwendung von vereinfachter Kommunikation installiert.

Der Agent erstellt Web-Socket-Verbindungen und sendet die Verbindungsdetails an alle Koordinationsrechner-Knoten. Koordinationsrechner verwenden diese Web-Socket-Verbindung, um bei Bedarf Anfragen oder Aktualisierungen an den Agenten zu senden.

Konfigurieren von Agenten zur Verwendung von veralteter Kommunikation

Agenten, die mit CA Process Automation 4.2 installiert werden, verwenden standardmäßig die vereinfachte Kommunikation. Bei Bedarf können Sie die Agentenkommunikation auf die veraltete Kommunikation zurücksetzen.

Wenn Sie eine Umgebung mit aktivierter Firewall verwenden, konfigurieren Sie die Verwendung der Firewall-Ports neu, bevor Sie von vereinfachter Kommunikation zu veralteter Kommunikation wechseln. Die Jetty-Ports, die für vereinfachte Kommunikation verwendet werden, sind die Standardports 80 für HTTP und 443 für HTTPS. Die Tomcat-Ports, die für veraltete Kommunikation verwendet werden, verwenden 8080 und 8443. Weitere Details zu Agentenports finden Sie im Thema "Von Agenten verwendete Ports" im *Installationshandbuch*.

Gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass der Agent ausgeführt wird.

   Wenn das Auswahlmenü "Agenten" einen CA Process Automation-Agenten als inaktiv anzeigt, können Sie den Agenten starten. Weitere Informationen finden Sie unter "So starten Sie einen Agenten oder halten ihn an".

2. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie die Option "Agenten" im Auswahlmenü "Konfigurationsbrowser".

3. Wählen Sie den Agenten aus, für den die Kommunikationen gewechselt werden sollen, und klicken Sie auf "Sperren".

4. Wählen Sie die Registerkarte "Eigenschaften" für den ausgewählten Agenten aus.

5. Wählen Sie das Kontrollkästchen "Veraltete Kommunikation verwenden" aus.

6. Wählen Sie den Agenten aus, und klicken Sie auf "Entsperren".
7. Klicken im Dialogfeld "Ungespeicherten Daten" auf "Ja", um die Änderungen zu speichern.

Der Agent beendet die Web-Socket-Verbindung. Nachdem die Web-Socket-Verbindung beendet wird, verwendet der Agent die veraltete Mitteilung.

Kapitel 9: Verwalten von Kontaktpunkten

Kontaktpunkte ordnen symbolische Namen zu Koordinationsrechnern und Agenten zu. Kontaktpunkte werden verwendet, um den Koordinationsrechner oder Agenten innerhalb einer Umgebung zu identifizieren. Eine Schicht wird zwischen CA Process Automation und der Netzwerktopologie bereitgestellt, damit CA Process Automation-Operatoren konfiguriert werden können, ohne ausdrücklich Hostinformation anzugeben.

Die Kategorienkonfiguration für einen Operator gibt den Kontaktpunkt an, auf dem der Operator ausgeführt werden soll. Ein Anwender, der einen CA Process Automation-Operator konfiguriert, wählt einen Namen aus einer Liste der Kontaktpunkte aus, die konfiguriert wurden, um die Operatoren in der gleichen Kategorie wie der referenzierte Operator auszuführen. Dieser Umweg ermöglicht es Ihnen, Hosts zur Laufzeit zu ersetzen. Der Umweg ermöglicht es Ihnen auch, mehrere CA Process Automation-Umgebungen zu definieren, in denen die gleichen Kontaktpunkte zu verschiedenen realen Hosts zugeordnet werden.

Dieses Kapitel enthält folgende Themen:

Kontaktpunkt-Implementierungs-Strategie

Ein *Kontaktpunkt* ist eine umgebungsspezifische logische Darstellung einer oder mehrerer verwalteter Ressourcen. Eine *verwaltete Ressource* ist ein Agent oder ein Koordinationsrechner, auf dem Operatoren eines Prozesses ausgeführt werden. Um einen Operator auf einem bestimmten Agenten oder seinem Failover-Agenten auszuführen, geben Sie als Ziel den Kontaktpunkt an, der diesen Agenten zugeordnet ist.

Inhaltsadministratoren erstellen Kontaktpunkte für Prozessziele in der Designumgebung, nachdem die Prozesspläne abgeschlossen sind, aber bevor der Designprozess startet. Inhaltsdesigner erstellen den Prozess, wobei Operatoren auf die von Ihnen erstellten Kontaktpunkte verweisen. Inhaltsdesigner testen den Prozess und verpacken ihn dann für die Übergabe in die Produktionsumgebung.

Bevor Sie den Prozess übergeben, erstellen Sie ähnliche Kontaktpunkte, die Produktionsagenten der Produktionsumgebung zuordnen. Erstellen Sie also die gleichen Kontaktpunktnamen oder Proxy-Kontaktpunktnamen in der Produktionsumgebung, die Sie in der Designumgebung verwendet haben. Durch die Erstellung dieser Kontaktpunkte können die Operatoren im übergebenen Prozess weiterhin die gleichen Kontaktpunkte wie die Operatorziele verwenden.

Betrachten Sie den folgenden Prozess:

1. Rufen Sie eine Testversion eines externen Systems oder eine Aktivität ab, die Sie als Ziel planen.

   Beispiele für externe Entitäten sind Service Desk-Anwendungen, eine Produktionsdatenbank oder ein Sicherungssystem.

2. Installieren Sie einen Agenten auf dem Host mit der Testversion der Entität, die Sie als Ziel planen.

   Wenn diese Vorgehensweise nicht möglich ist, erstellen Sie eine SSH-Verbindung von einem Agentenhost zum Host mit dem Ziel, und erstellen Sie dann einen Proxy-Kontaktpunkt.

3. Ordnen Sie dem Agenten in der Designumgebung, auf der die Testkopie des vorgesehenen externen Systems ausgeführt wird, einen Kontaktpunkt (oder Proxy-Kontaktpunkt) zu.

4. Designer führen den Prozess aus und testen ihn, wobei Operatoren im Prozess auf den Kontaktpunkt für das Testen verweisen.

5. Führen Sie während der Übergabe eines Prozesses zur Produktionsumgebung den folgenden Vorgang für jedes Ziel aus, das ein Agentenkontaktpunkt ist:

   a. Identifizieren Sie die Hosts, auf denen die Anwendung, die Datenbank oder das System, auf die bzw. das verwiesen werden soll, ausgeführt werden.

   b. Installieren Sie einen Agenten auf jedem identifizierten Host.

   c. Erstellen Sie einen Kontaktpunkt, der jeden Agenten, der ein mögliches Ziel darstellt, der Produktionsumgebung zuordnet. Benennen Sie den Kontaktpunkt mit dem gleichen Namen, der in der Designumgebung verwendet wird.

6. Führen Sie während der Übergabe eines Prozesses den folgenden Vorgang für jedes Ziel aus, das ein Proxy-Kontaktpunkt ist:

   a. Identifizieren Sie den Remote-Host, der die Anwendung, die Datenbank oder das System, auf die bzw. das verwiesen werden soll, ausführt.

   b. Installieren Sie einen Agenten auf einem verfügbaren Host.

   c. Erstellen Sie eine SSH-Verbindung vom Agentenhost zum Remote-Host.

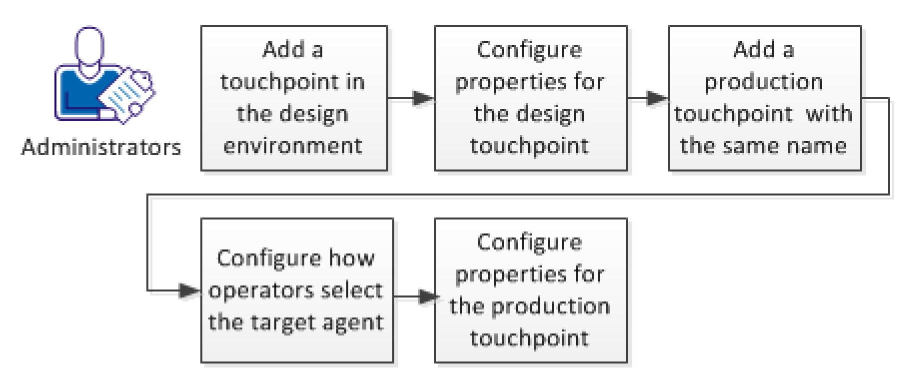
   d. Erstellen Sie einen Proxy-Kontaktpunkt, der den Agentenhost zur Produktionsumgebung zuordnet. Benennen Sie den Proxy-Kontaktpunkt mit dem gleichen Namen, der für den Proxy-Kontaktpunkt in der Designumgebung verwendet wurde.

Einrichten von Kontaktpunkten für Design und Produktion

Ein Operator, der einen Kontaktpunkt als Ziel hat, kann sowohl in der Designumgebung als auch in der Produktionsumgebung ausgeführt werden, ohne, dass Änderungen am Feld "Ziel" des Operators vorgenommen werden müssen. Um dies zu ermöglichen, definieren Sie in beiden Umgebungen den gleichen Kontaktpunktnamen.

Sie können Kontaktpunkte für Design und Produktion einrichten, wenn Sie folgende Voraussetzungen fertiggestellt haben:

- Installieren Sie Agenten auf Hosts, die Ziele des Prozesses sein sollen, in der Designumgebung.
- Installieren Sie Agenten auf Hosts, die Ziele des Prozesses sein sollen, in der Produktionsumgebung.



Gehen Sie folgendermaßen vor:

1. Hinzufügen von Kontaktpunkten in der Designumgebung (siehe Seite 238).
2. Konfigurieren von Eigenschaften für den Designkontaktpunkt (siehe Seite 238).
3. Hinzufügen eines Produktions-Kontaktpunkts mit demselben Namen (siehe Seite 239).
4. Konfigurieren der Auswahl des Ziel-Agenten durch Operatoren (siehe Seite 241).
5. Konfigurieren von Eigenschaften für den Produktionskontaktpunkt (siehe Seite 242).

Hinzufügen von Kontaktpunkten in der Designumgebung

Ein Kontaktpunkt ordnet einen Agenten einer Umgebung zu. Sie können einen Kontaktpunkt hinzufügen und ihn zu einem Agenten zuordnen, der auf einem Host installiert ist, der während Design und Test als Ziel verwendet werden soll.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie im Konfigurationsbrowser Domäne ein.
3. Wählen Sie die Umgebung aus, die Sie für das Design verwenden, und klicken Sie auf Sperren.
4. Klicken Sie mit der rechten Maustaste auf die Umgebung, und klicken Sie auf Kontaktpunkt hinzufügen.
5. Geben Sie im Feld Kontaktpunktname im Dialogfeld Kontaktpunkt hinzufügen: *Umgebung* einen Namen für den neuen Kontaktpunkt ein.
6. Wählen Sie den Agenten aus, der auf dem Host installiert ist, der das Ziel dieses Kontaktpunkts sein soll.
7. Klicken Sie auf Hinzufügen, klicken Sie in der Menüleiste auf Speichern, klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie Entsperren aus.
8. Zeigen Sie die hinzugefügten Kontaktpunkte im Knoten Alle Kontaktpunkte der Designumgebung an. Zeigen Sie die zusätzliche Zeile in der Registerkarte Kontaktpunktdaten an.

Konfigurieren von Eigenschaften für den Design-Kontaktpunkt

Sie konfigurieren Eigenschaften für einen Kontaktpunkt basierend auf der Umgebung. Für Kontaktpunkte, die zu einer Designumgebung zugeordnet sind, haben Sie die Option, Operatoren manuell wiederherzustellen. Diese Einstellung ist am Besten für die Fehlerbehebung geeignet. Kontaktpunktsicherheit zielt üblicherweise auf essenziell wichtige Hosts ab und ist im Normalfall nicht für Agenten-Hosts anwendbar, die während des Designs verwendet werden.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie mit der rechten Maustaste auf die Umgebung mit den Kontaktpunkten, die konfiguriert werden sollen, und wählen Sie Sperren aus.
3. Blenden Sie die Umgebung ein, und erweitern Sie Alle Kontaktpunkte.
4. Wählen Sie den Kontaktpunkt aus, der konfiguriert werden soll, und klicken Sie auf die Registerkarte Eigenschaften.

5. Legen Sie die Eigenschaft "Automatische Wiederherstellung von Operatoren" so fest, dass Sie Operatoren manuell wiederherstellen können. Diese Einstellung verleiht Ihnen bei Bedarf optimale Kontrolle über die Wiederherstellung von Operatoren.
6. Wenn dieser Kontaktpunkt durch eine aktive Richtlinie für Kontaktpunktsicherheit geschützt wird, aktivieren Sie die Eigenschaft Kontaktpunktsicherheit.

   Das Aktivieren der Eigenschaft setzt die anwendbare Richtlinie durch, in der die Anwender angegeben sind, die Operatoren auf dem aktuellen Ziel ausführen dürfen.
7. Klicken Sie auf "Speichern".
8. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie Entsperren aus.

Hinzufügen eines Produktions-Kontaktpunkts mit demselben Namen

Wenn Inhaltsdesigner Kontaktpunktnamen für Operatoren ins Feld "Ziel" eingeben, wird der Operator auf dem Agenten ausgeführt, der zum Kontaktpunkt in der Designumgebung zugeordnet ist.

Ein Kontaktpunktname muss innerhalb einer Umgebung eindeutig sein. Zwei Umgebungen können verschiedene Kontaktpunkte mit demselben Namen haben. Folgendes Szenario ist gültig, wo zwei verschiedene Kontaktpunkte mit dem Namen "TP-125" vorhanden sind.

- "TP-125" wird "agent-1" und der Designumgebung zugeordnet
- "TP-125" wird "agent-2" und der Produktionsumgebung zugeordnet

Agenten sind nicht umgebungsspezifisch. Sie können zwei Kontaktpunkte mit demselben Namen in unterschiedlichen Umgebungen zum selben Agenten zuordnen.

Wenn ein Prozess in eine andere Umgebung übertragen wird, muss jeder Operator auf einem Agenten ausgeführt werden, der in der Importumgebung verwendet wird. Um sich auf die Verwendung eines importierten Prozesses vorzubereiten, führen Sie die folgenden Aktionen durch:

1. Identifizieren Sie die einzelnen Kontaktpunkte, die von einem Operator in einem Prozess, der in der Designumgebung ausgeführt wird, als Ziel verwendet werden sollen. Der Prozess kann sich in der Planungsstufe befinden oder für den Export bereit sein.
2. Bestimmen Sie für jeden identifizierten Kontaktpunkt zwei passende Agenten, die in der Produktionsumgebung verwendet werden, in der der Operator ausgeführt werden kann. Für Hochverfügbarkeitszwecke wird empfohlen, zwei Agenten anstelle eines einzelnen zuzuordnen.
3. Erstellen Sie in der Produktionsumgebung einen Kontaktpunkt mit demselben Namen wie der identifizierte Kontaktpunkt. Ordnen Sie ihn zu den entsprechenden Agenten zu, die in der Produktionsumgebung verwendet werden. Der folgende Vorgang beschreibt diesen Schritt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie im Auswahlmenü Konfigurationsbrowser mit der rechten Maustaste auf die Produktionsumgebung, und klicken Sie auf Sperren.
3. Klicken Sie mit der rechten Maustaste auf die Produktionsumgebung, und klicken Sie auf Kontaktpunkt hinzufügen.
4. Geben Sie denselben Kontaktpunktnamen ein, der in der Designumgebung verwendet wird. Geben Sie den Namen ins Feld Kontaktpunktname im Dialogfeld Kontaktpunkt hinzufügen:*Produktionsumgebung* ein.
5. Wählen Sie die beiden zuvor identifizierten Agenten aus, die als Ziele dieses Kontaktpunkts verwendet werden sollen.
6. Klicken Sie auf Hinzufügen, klicken Sie in der Menüleiste auf Speichern, klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie Entsperren aus.
7. Zeigen Sie die hinzugefügten Kontaktpunkte im Knoten Alle Kontaktpunkte der Designumgebung an. Zeigen Sie die zusätzliche Zeile in der Registerkarte Kontaktpunktdaten an.

Hinweis: Wenn Sie zum Kontaktpunkt in der Zielumgebung mehrere Agenten zugeordnet haben, müssen Sie konfigurieren, wie Operatoren den Zielagenten auswählen.

Weitere Informationen:

Konfigurieren der Auswahl des Ziel-Agenten durch Operatoren (siehe Seite 241)

Konfigurieren der Auswahl des Ziel-Agenten durch Operatoren

Sie können mehrere Agenten zum gleichen Kontaktpunkt zuordnen. Wenn ein Operator auf solch einen Kontaktpunkt abzielt, kann der Operator einen bestimmten Agenten auswählen oder einen Agenten nach dem Zufallsprinzip auswählen. Standardmäßig wählt der Operator den ersten Agenten aus, den Sie dem Kontaktpunkt zugeordnet haben.

Sie können konfigurieren, wie Operatoren den Agenten für die Ausführung auswählen.

- Um Operatoren anzuweisen, Ihren bevorzugten Agenten auszuwählen, weisen Sie diesem Agenten Priorität 1 zu. Weisen Sie dem Backup-Agenten Priorität 2 zu.
- Um Operatoren anzuweisen, den Agenten nach dem Zufallsprinzip auszuwählen, weisen Sie allen Agenten Priorität 1 zu.

Sie können konfigurieren, wie Operatoren den Zielhost auswählen, indem Sie den zugeordneten Agenten Prioritäten zuweisen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie die Domäne, wählen Sie die zu konfigurierende Umgebung aus, und klicken Sie auf "Sperren".
3. Erweitern Sie die Umgebung. Klicken Sie unter "Alle Kontaktpunkte" auf den Agentenkontaktpunkt, den Sie konfigurieren möchten.

   Auf der Registerkarte "Agenten" wird die Liste der Agenten angezeigt, die dem ausgewählten Kontaktpunkt zugeordnet sind. Jeder Agent wird mit einem Prioritätswert aufgelistet, der die Reihenfolge widerspiegelt, in der er hinzugefügt wurde.
4. Überprüfen Sie die angezeigten Prioritätseinstellungen, und führen Sie eine der folgenden Aktionen durch:
   - Weisen Sie für den Lastenausgleich die gleiche Zahl jedem Agenten zu, der potenziell der aktive Agent sein kann. Weisen Sie zum Beispiel "1" zu.
   - Weisen Sie für Backup dem Agenten "1" zu, um auf den Kontaktpunkt zu verweisen. Weisen Sie dem Backup-Agenten, der nur dann den Betrieb übernehmen soll, wenn der Agent mit der hohen Priorität inaktiv wird, "2" zu.
   - Weisen Sie beiden Agenten, die am Lastenausgleich teilnehmen sollen, "1" zu, und weisen Sie dem Agenten oder den Agenten, die als Backups fungieren sollen, eine höhere Nummer zu.
5. Klicken Sie auf "Speichern".
6. Wählen Sie die Umgebung aus, und klicken Sie dann auf "Entsperren".

Konfigurieren von Eigenschaften für den Produktionskontaktpunkt

Sie können Eigenschaften für einen Kontaktpunkt basierend auf der zugeordneten Umgebung konfigurieren. In einer Produktionsumgebung reduziert das Aktivieren von "Automatische Operator-Wiederherstellung" die Zeit, die dafür beansprucht wird, die Ausführung eines Prozesses wiederherzustellen, wenn ein Operator mit wiederherstellbaren Prozessen fehlschlägt. Kontaktpunktsicherheit wird nur bei sehr wichtigen Hosts in der Produktionsumgebung angewendet. Legen Sie deswegen diese Eigenschaft je nachdem fest, ob diesem Kontaktpunkt eine Richtlinien für Kontaktpunktsicherheit zugeordnet ist, die die ihm zugeordneten Agenten schützt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie mit der rechten Maustaste auf die Umgebung mit den Kontaktpunkten, die konfiguriert werden sollen, und wählen Sie Sperren aus.
3. Blenden Sie die Umgebung ein, und erweitern Sie Alle Kontaktpunkte.
4. Wählen Sie den Kontaktpunkt aus, der konfiguriert werden soll, und klicken Sie auf die Registerkarte Eigenschaften.
5. Legen Sie die Eigenschaft Automatische Operator-Wiederherstellung fest, damit Operatoren automatisch wiederhergestellt werden.

   Diese Einstellung vermindert die Auswirkung von Netzwerkproblemen auf Produktionsanwender.
6. Wenn die Produktionsagenten, die zu diesem Kontaktpunkt zugeordnet sind, in einer Richtlinie für Kontaktpunktsicherheit definiert sind, aktivieren Sie die Eigenschaft Kontaktpunktsicherheit.

   Das Aktivieren der Eigenschaft setzt die anwendbare Richtlinie durch, in der die Anwender angegeben sind, die Operatoren auf diesen Agenten ausführen dürfen.
7. Klicken Sie auf "Speichern".
8. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie Entsperren aus.

Hinzufügen eines oder mehrerer Kontaktpunkte

Sie können Kontaktpunkte gleichzeitig hinzufügen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie im Konfigurationsbrowser Domäne ein.
3. Klicken Sie mit der rechten Maustaste auf die Umgebung, die konfiguriert werden soll, und klicken Sie auf Sperren.

4. Klicken Sie mit der rechten Maustaste auf die Umgebung, und klicken Sie auf Kontaktpunkt hinzufügen.
5. Geben Sie im Feld Kontaktpunktname im Dialogfeld Kontaktpunkt hinzufügen: *Umgebung* einen Namen für den neuen Kontaktpunkt ein.
6. Wählen Sie aus der Drop-down-Liste ein Objekt aus, das dem Kontaktpunkt zugeordnet werden soll. Wählen Sie Folgendes aus:
   - Einen Koordinationsrechner
   - Einen Agenten
   - Mehrere Agenten
7. Klicken Sie auf Hinzufügen, klicken Sie in der Menüleiste auf Speichern, klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie Entsperren aus.
8. Zeigen Sie die hinzugefügten Kontaktpunkte im Knoten Alle Kontaktpunkte der ausgewählten Umgebung an. Zeigen Sie die zusätzliche Zeile in der Registerkarte Kontaktpunktdaten an.

Hinzufügen eines oder mehrere Agenten zu einem vorhandenen Kontaktpunkt

Sie können einen oder mehrere Agenten zu einem vorhandenen Kontaktpunkt hinzufügen. Wir empfehlen, dass Sie jedem Kontaktpunkt, den Sie zu Ihrer Produktionsumgebung zuordnen, mehr als einen Agenten hinzufügen. Wenn ein Agent nicht verfügbar ist, kann ein Operator, der auf den Kontaktpunkt zielt, auf einem anderen zugeordneten Agenten ausgeführt werden.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie den Knoten "Domäne" im Auswahlmenü "Konfigurationsbrowser" ein, wählen Sie eine Umgebung aus, und klicken Sie dann auf "Sperren".

3. Wenn ein Kontaktpunkt nicht vorhanden ist, dann erstellen Sie einen:
   a. Erweitern Sie den Knoten "Agenten".
   b. Identifizieren Sie einen Agenten, der in der gesperrten Umgebung ausgeführt wird. Klicken Sie mit der rechten Maustaste auf den Agenten, wählen Sie "Kontaktpunkt konfigurieren in" aus, und wählen Sie anschließend die gesperrte Umgebung aus.

      Das Dialogfeld Agentenkontaktpunkt hinzufügen wird angezeigt.
   c. Geben Sie den Namen des entsprechenden Kontaktpunkts ein, und klicken Sie auf OK.
4. Um einen oder mehrere Agenten zu einem vorhandenen Kontaktpunkt hinzufügen, gehen Sie folgendermaßen vor:
   a. Blenden Sie "Alle Kontaktpunkte" für die ausgewählte Umgebung ein, wählen Sie den Zielkontaktpunkt aus, und klicken Sie dann auf "Hinzufügen".
   b. Wählen Sie einen oder mehrere aktive Agenten aus, die in der gesperrten Umgebung ausgeführt werden, und klicken Sie auf "Hinzufügen". (Die aktiven Agenten werden in Grün angezeigt.)

      Die neuen Agenten, die dem ausgewählten Kontaktpunkt zugeordnet werden sollen, werden in der Liste auf der Registerkarte Agenten angezeigt.
   c. Klicken Sie auf "Speichern".

      Der ausgewählte Kontaktpunkt ist nun zu den zusätzlichen Agenten zugeordnet.
5. Klicken Sie mit der rechten Maustaste auf die gesperrte Umgebung, und wählen Sie Entsperren aus.
6. Klicken Sie in der Aufforderung zum Speichern von Änderungen auf Ja.

Hinweis: Wenn Sie zum Kontaktpunkt in der Zielumgebung mehrere Agenten zugeordnet haben, müssen Sie konfigurieren, wie Operatoren den Zielagenten auswählen.

Weitere Informationen:

Konfigurieren der Auswahl des Ziel-Agenten durch Operatoren (siehe Seite 241)

Gebündeltes Hinzufügen von Kontaktpunkten für Agenten

Sie können Kontaktpunkte zu neuen Agenten gebündelt hinzufügen, indem Sie Muster für Hostnamen oder IP-Adressen der Agenten angeben. Jeder Agent mit einem Hostnamen oder einer IP-Adresse, der mit dem angegebenen Muster übereinstimmt, wird automatisch mit einem Kontaktpunkt konfiguriert. Der Kontaktpunktname ist identisch mit dem Anzeigenamen des Agenten. Ein *automatisch zuzulassendes Muster* ist ein als regulärer Ausdruck ausgedrücktes Hostnamensmuster oder ein in CIDR-Notation ausgedrücktes IP-Adressensubnetz.

Sie können für jede Umgebung eigene Muster für die automatische Zulassung konfigurieren oder umgebungsübergreifend dieselben oder überlappende Muster für die automatische Zulassung konfigurieren. Kontaktpunkte sind umgebungsspezifisch. Bei Agenten ist dies nicht der Fall.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie im "Konfigurationsbrowser" die Option "Domäne" ein.
3. Klicken Sie mit der rechten Maustaste auf die Umgebung, die Sie konfigurieren möchten, und klicken Sie dann auf "Sperren".
4. Klicken Sie auf die Registerkarte "Auto-Admit".
5. Gehen Sie für jedes IP-Adress-Muster folgendermaßen vor. Verwenden Sie die Auf- und Abwärtspfeile, um die Suchliste zu ordnen.
   a. Klicken Sie im Feld "IP-Adressmuster" auf "Hinzufügen".

      Ein Eingabefeld wird angezeigt.

   b. Geben Sie mithilfe der CIDR-Notation ein IPv4-Subnetz ein.

      Hinweis: In CA Process Automation wird der CIDR-Mustervergleich für Anforderungen zur automatischen Zulassung verwendet. Das CIDR-Muster 155.32.45.0/24 stimmt beispielsweise mit IP-Adressen im Bereich von 155.32.45.0 bis 155.32.45.255 überein.

6. Gehen Sie für jedes Host-Namensmuster folgendermaßen vor. Verwenden Sie die Auf- und Abwärtspfeile, um die Suchliste zu ordnen.
   a. Klicken Sie im Feld "Host-Namensmuster" auf "Hinzufügen".
   b. Geben Sie ein Host-Namensmuster ein.

      Hinweis: Der Hostname des Koordinationsrechners/Agenten wird mit den angegebenen regulären Ausdrücken verglichen. Wenn das angegebene Muster beispielsweise "ca\.com$" lautet, werden alle Agenten/Koordinationsrechner hinzugefügt, deren Hostname auf "ca.com" endet.

7. Klicken Sie mit der rechten Maustaste auf die Umgebung, und klicken Sie dann auf "Entsperren".
8. Wiederholen Sie diesen Vorgang für jede Umgebung.

   Die Domäne sucht nach einem neuen Koordinationsrechner und neuen Agenten mit IP-Adressen oder Hostnamen, die mit den Mustern für die automatische Zulassung für eine oder mehrere Umgebungen übereinstimmen.

   Wenn die Domäne solche neuen Agenten erkennt, erstellt die Domäne einen Kontaktpunkt für jede Übereinstimmung und fügt ihn automatisch jeder Umgebung hinzu. Der Name des Kontaktpunkts ist der Anzeigename des Agenten.

   Wenn die Domäne einen solchen Koordinationsrechner erkennt, erstellt die Domäne einen Kontaktpunkt für diesen Koordinationsrechner und fügt ihn der ersten übereinstimmenden Umgebung hinzu. Ein Koordinationsrechner hat nur einen Kontaktpunkt.

Beispiel für Kontaktpunkte, die Umgebungen auf der Basis von Mustern für die automatische Zulassung von Agenten hinzugefügt werden

Im folgenden Beispiel werden für zwei Umgebungen überlappende Muster für die automatische Zulassung definiert. Es werden zwei Agenten installiert, wobei die IP-Adresse des einen Agenten mit dem automatisch zuzulassenden Muster in einer Umgebung übereinstimmt und die IP-Adresse des anderen Agenten mit dem automatisch zuzulassenden Muster in beiden Umgebungen übereinstimmt. Das Ergebnis besteht darin, dass automatisch drei Kontaktpunkte hinzugefügt werden.

- Das Muster für die automatische Zulassung von Umgebung1 lautet 155.32.45.0/24 (155.32.45.0 - 155.32.45.255).
- Das Muster für die automatische Zulassung von Umgebung2 lautet 155.32.45.32/27 (155.32.45.32 - 155.32.45.63).
- Es werden neue Agenten mit den folgenden Adressen installiert:
  - 155.32.45.5 mit dem Anzeigenamen "host1.mycompany.com"
  - 155.32.45.50 mit dem Anzeigenamen "host2.mycompany.com"

Die folgenden Kontaktpunkte werden auf der Basis der Muster für die automatische Zulassung automatisch hinzugefügt:

- Kontaktpunktname: host1.mycompany.com in Umgebung1
- Kontaktpunktname: host2.mycompany.com in Umgebung1
- Kontaktpunktname: host2.mycompany.com in Umgebung2

Verbinden eines Kontaktpunkts mit einem anderen Agenten

Verbinden Sie einen vorhandenen Kontaktpunkt mit einem anderen Agenten in Fällen wie den Folgenden:

- Ein Prozess wird regelmäßig auf einem für das Entfernen aus dem Netzwerk geplanten Host ausgeführt.

  Hier wird der Kontaktpunkt mit nur einem Agenten verbunden, und dieser Agent wird auf einem Host installiert, der stillgelegt werden soll. Wenn ein Kontaktpunkt zu mehreren Agenten zugeordnet ist, dann ist keine Aktion erforderlich.

- Ein Prozess, der in einem Rechenzentrum ausgeführt wurde, muss jetzt in einem anderen Rechenzentrum ausgeführt werden.

  Hier verweist der Prozess auf einen Kontaktpunkt, der mit einem auf einem Host installierten Agenten im neuen Rechenzentrum verbunden sein muss.

Das Ändern der Agentenverbindung für einen ausgewählten Kontaktpunkt umfasst das Löschen der aktuellen Agentenverbindung und das anschließende Hinzufügen einer neuen Agentenverbindung. Um einen getesteten Prozess auf mehreren Hosts auszuführen, verbinden Sie den gleichen referenzierten Kontaktpunkt mit dem Agenten, der auf jedem Zielhost ausgeführt wird.

Sie können die Agentenverbindung für einen angegebenen Kontaktpunkt ersetzen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie die Struktur, um Alle Kontaktpunkte anzuzeigen, und wählen Sie den Zielkontaktpunkt aus.

   Auf der Registerkarte Agenten werden die Agenten aufgelistet, die derzeit mit dem ausgewählten Kontaktpunkt verbunden sind.

3. Wählen Sie den Agenten aus, mit dem Sie die Vereinigung auflösen möchten, und klicken Sie auf Löschen.
4. Wenn die Meldung für die Löschbestätigung angezeigt wird, klicken Sie auf OK.

   Der Agentenkontaktpunkt wird aus der Liste entfernt.

5. Klicken Sie auf Hinzufügen.

   "Agentenreferenz hinzufügen zu: *Kontaktpunktname*" wird mit einer Liste aller Agenten angezeigt. Aktive Agenten werden in Grün angezeigt.

6. Wählen Sie einen oder mehrere aktive Agenten aus, und klicken Sie auf Hinzufügen.

   Der neue Agent, der mit dem ausgewählten Kontaktpunkt verbunden werden soll, wird in der Liste auf der Registerkarte "Agenten" angezeigt.

7. Klicken Sie auf "Speichern".

   Der ausgewählte Kontaktpunkt ist jetzt mit einem anderen Agenten verbunden.

Löschen eines Kontaktpunkts

Sie können Kontaktpunkte löschen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie die Domäne und die Umgebung mit dem Kontaktpunkt.
3. Klicken Sie mit der rechten Maustaste auf die Umgebung mit dem Kontaktpunkt, und klicken Sie auf Sperren.
4. Erweitern Sie Alle Kontaktpunkte, und wählen Sie den Kontaktpunkt aus, den Sie löschen möchten.

   Die Registerkarte "Agenten" wird geöffnet und listet die Agenten auf, die zu dem Kontaktpunkt zugeordnet sind.
5. Wählen Sie alle Agenten aus, die zum Kontaktpunkt zugeordnet sind, und klicken Sie auf "Löschen".

   Eine Bestätigungsmeldung wird angezeigt.
6. Klicken Sie auf Ja.

   Der gelöschte Kontaktpunkt wird aus der Liste Alle Kontaktpunkte der Registerkarte Kontaktpunktdaten entfernt.
7. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Gebündeltes Entfernen nicht verwendeter leerer Kontaktpunkte

Wenn Agenten gebündelt entfernt werden, können leere Kontaktpunkte erstellt werden. Wenn diese Kontaktpunkte in aktiven Prozessen verwendet werden, weisen Sie sie anderen Agenten zu.

Sie können Kontaktpunkte auf zwei Ebenen entfernen:

- Um ausgewählte Kontaktpunkte umgebungsübergreifend zu entfernen, initiieren Sie die Entfernung über das Kontextmenü der Domäne.

  Sie müssen über Inhaltsadministrator- und Domänenadministratorrechte verfügen.
- Um ausgewählte Kontaktpunkte innerhalb einer Umgebung zu entfernen, initiieren Sie die Entfernung über das Kontextmenü der Umgebung.

  Sie müssen über Inhaltsadministratorrechte für die ausgewählte Umgebung verfügen, um ihre Kontaktpunkte entfernen zu können.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Sperren Sie die Domäne oder die Zielumgebung. Wenn diese bereits mit noch nicht gespeicherten Änderungen gesperrt ist, speichern Sie die Änderungen.
3. Klicken Sie mit der rechten Maustaste auf die Domäne oder die Zielumgebung, und wählen Sie Gebündelte Entfernung von Kontaktpunkten aus.

   Das Dialogfeld "Gebündelte Entfernung von Kontaktpunkten" wird angezeigt.
4. Klicken Sie auf Suchen oder geben Sie einen Ausdruck für die Suche nach dem Kontaktpunktnamen ein, und klicken Sie auf Suchen.

   Die zurückgegebene Liste enthält nur den Namen und den Zustand leerer Kontaktpunkte, die mit Ihren Suchkriterien übereinstimmen. Wenn Sie die Entfernung auf der Domänenebene initiiert haben, wird zudem die Umgebung für jeden Kontaktpunkt gezeigt.
5. Wählen Sie aus der angezeigten Liste mit Kontaktpunkten, die keinen Agenten zugeordnet, sind die Kontaktpunkte aus, die gelöscht werden sollen, und klicken Sie auf Löschen.

   In einer Bestätigungsmeldung wird die Anzahl der für die Löschung vorgesehenen Kontaktpunkte angegeben.
6. Prüfen Sie die Meldung.
   - Wenn die angezeigte Anzahl der Anzahl entspricht, die Sie auswählen wollten, klicken Sie auf Fortfahren, um diese Kontaktpunkte zu entfernen.
   - Wenn bei der Auswahl ein Fehler aufgetreten ist, klicken Sie auf Abbrechen, und wiederholen Sie die Schritte 4 und 5.

Umbenennen eines Kontaktpunkts

Das Umbenennen eines Kontaktpunkts ist nur dann mit Voraussetzungen verbunden, wenn der Operator "Programm ausführen" oder "Skript ausführen" auf dem Kontaktpunkt ausgeführt wird.

Wichtig! Der Operator "Programm ausführen" und der Operator "Skript ausführen" in der Kategorie "Befehlsausführung" verweisen auf Kontaktpunkte direkt über den Namen. Aktualisieren Sie daher die Referenzen zum Kontaktpunkt im Operator "Programm ausführen" und im Operator "Skript ausführen", bevor Sie den Kontaktpunkt umbenennen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", und erweitern Sie die Option "Domäne" im Auswahlmenü "Konfigurationsbrowser".
2. Wählen Sie die geeignete Umgebung aus, und klicken Sie auf "Sperren".

3. Blenden Sie Alle Kontaktpunkte ein.
4. Klicken Sie mit der rechten Maustaste auf den geeigneten Kontaktpunkt, und klicken Sie auf "Umbenennen".
5. Geben Sie den neuen Kontaktpunktnamen des Agenten ein.

   Hinweis: Das Symbol für ungespeicherte Daten wird links von Ihrer Eingabe als Erinnerung angezeigt, damit Sie Ihre Änderungen speichern. Klicken Sie auf "Speichern", oder warten Sie auf die Textaufforderung.
6. Wählen Sie die Umgebung aus, die Sie gesperrt haben, und klicken Sie auf Entsperren.

   Im Dialogfeld Nicht gespeicherte Daten werden Sie aufgefordert, die Änderungen zu speichern.
7. Klicken Sie auf Ja.

Verwalten von Kontaktpunktgruppen

Jeder Kontaktpunkt ist ein Mitglied der Standardgruppe "Alle Kontaktpunkte". Sie können zusätzlich Ihre eigenen benannten Gruppen erstellen, um Kontaktpunkte nach Funktion oder logisch zu gruppieren. Die logische Gruppierung von Kontaktpunktgruppen ermöglicht es Ihnen, verwandte Kontaktpunkte zu organisieren und Kontaktpunkte in einer Umgebung leichter zu durchsuchen.

Die Gruppierung von Kontaktpunktgruppen nach Funktion ermöglicht, dass Befehle und Operatoren auf allen Kontaktpunkten in der Gruppe operieren können:

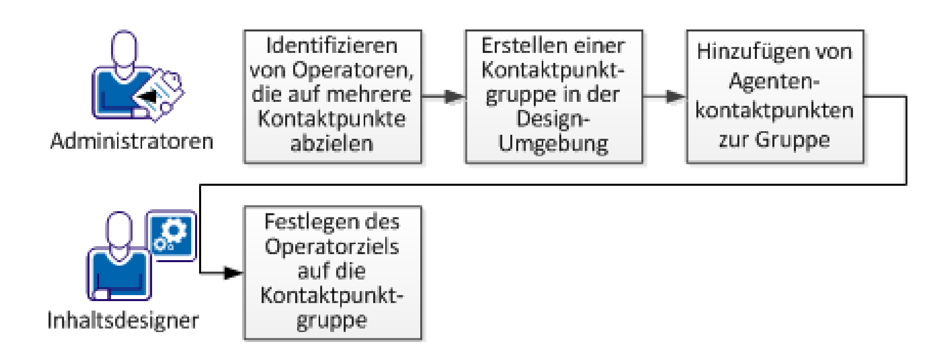
- Der für eine Kontaktpunktgruppe ausgeführte Befehl "Erneut laden" aktualisiert die Kontaktpunktliste für alle Kontaktpunkte in der Gruppe.
- Der für eine Kontaktpunktgruppe ausgeführte Befehl "Aktualisieren" aktualisiert Eigenschaftseinstellungen für alle Kontaktpunkte in der Gruppe.
- Ein Operator, der konfiguriert wurde, um zur Laufzeit für eine Gruppe ausgeführt zu werden, wird für jeden Kontaktpunkt in der Gruppe ausgeführt.

Eine Kontaktpunktgruppe ist aktiv, wenn mindestens ein Kontaktpunkt in der Gruppe aktiv ist. Eine Kontaktpunktgruppe ist inaktiv, wenn alle Kontaktpunkte in der Gruppe inaktiv sind. Wenn alle Kontaktpunkte in einer Gruppe aktiv sind, ist das Kontaktpunktgruppen-Symbol grün. Wenn einige Kontaktpunkte aktiv sind, ist das Kontaktpunktgruppen-Symbol gelb. Wenn alle Kontaktpunkte in einer Gruppe inaktiv sind, ist das Kontaktpunktgruppen-Symbol rot.

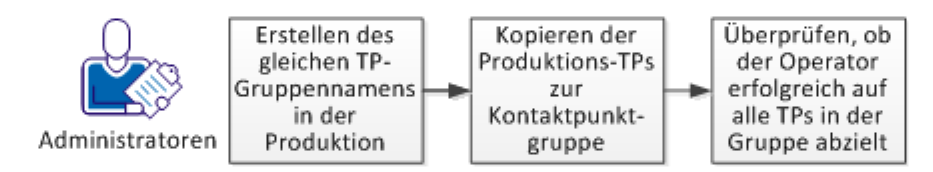
Ein Anwender muss Umgebungsadministratorrechte haben, um eine Kontaktpunktgruppe in einer Umgebung zu erstellen.

Informationen zu Kontaktpunktgruppen

Wenn ein bestimmter Operator gleichzeitig auf mehrere Kontaktpunkte abzielen muss, erstellen Administratoren eine Kontaktpunktgruppe, die als Operatorziel dienen kann. Zum Beispiel:



Wenn Administratoren ein Ziel der Kontaktpunktgruppe zur Produktionsumgebung übertragen, erstellen sie eine Kontaktpunktgruppe in der Produktionsumgebung. Der Kontaktpunktname dupliziert den Namen, der in der Designumgebung verwendet wird. Administratoren ordnen die Produktionsagenten und Koordinationsrechner zur Kontaktpunktgruppe zu. Wenn sie den Prozess testen, wird unter anderem überprüft, ob Operatoren, die auf eine Kontaktpunktgruppe verweisen, tatsächlich auf jedem Koordinationsrechner und Agenten ausgeführt werden, die durch einen Kontaktpunkt in dieser Gruppe dargestellt werden. Zum Beispiel:



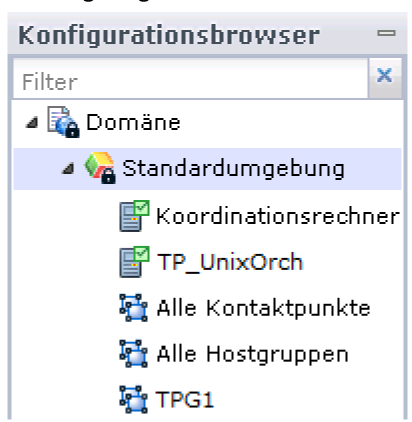
Erstellen einer Kontaktpunktgruppe mit ausgewählten Kontaktpunkten

Erstellen Sie eine Kontaktpunktgruppe, die als Operatorziel dienen kann, wenn ein bestimmter Operator gleichzeitig auf mehrere Kontaktpunkte abzielen muss. Sie fügen eine Kontaktpunktgruppe auf Umgebungsebene hinzu. Wählen Sie jeden Kontaktpunkt für die Gruppe aus der Domänenhierarchie aus. Sie können einen Koordinationsrechner- oder Agentenkontaktpunkt auswählen und dann die Option "Kopieren zu" verwenden, um einen ausgewählten Kontaktpunkt zu einer Kontaktpunktgruppe zu kopieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie die Domäne, wählen Sie die Umgebung aus, die sie konfigurieren wollen, und klicken Sie auf Sperren.
3. Erstellen Sie eine Kontaktpunktgruppe:
   a. Klicken Sie mit der rechten Maustaste auf eine Umgebung, und wählen Sie Neue Gruppe hinzufügen aus.
   b. Geben Sie im Dialogfeld Kontaktpunktgruppe hinzufügen einen Namen für die neue Kontaktpunktgruppe ein, und klicken Sie auf OK.

      Wenn Sie beispielsweise "TPG1" als Namen eingeben, wird der neue Gruppenname unter der ausgewählten Umgebung unter Alle Hostgruppen angezeigt.



   c. Klicken Sie auf "Speichern".

      Hinweis: Sie können einen Koordinationsrechner nicht erfolgreich zu einer nicht gespeicherten Kontaktpunktgruppe hinzufügen.

4. Kopieren Sie Koordinationsrechner- und Agentenkontaktpunkte zur Kontaktpunktgruppe. Zum Beispiel:

   a. Klicken Sie mit der rechten Maustaste auf einen Koordinationsrechner, und wählen Sie Kopieren zu, *Gruppenname* aus.

      Der ausgewählte Koordinationsrechner wird in der Hierarchie unter dem ausgewählten Kontaktpunktgruppennamen angezeigt.

   b. Klicken Sie auf "Speichern".

   c. Klicken Sie mit der rechten Maustaste auf einen anderen Koordinationsrechner, wählen Sie Kopieren zu aus, und wählen Sie dann den gleichen *Gruppennamen* aus.

   d. Klicken Sie auf "Speichern".

   e. Erweitern Sie Alle Kontaktpunkte, klicken Sie mit der rechten Maustaste auf einen Agentenkontaktpunkt, wählen Sie Kopieren zu aus, und wählen Sie den gleichen *Gruppennamen* aus.

   Die Kontaktpunktgruppe "TPG1" zeigt Inhalte von zwei Koordinationsrechner-Kontaktpunkten und einem Agentenkontaktpunkt im folgenden Beispiel an:



5. Wählen Sie die Umgebung aus, und wählen Sie Entsperren aus.

   Im Dialogfeld Nicht gespeicherte Daten werden Sie aufgefordert, die Änderungen zu speichern.

6. Klicken Sie auf Ja.

Weitere Informationen:

Verwalten von Kontaktpunktgruppen (siehe Seite 250)

Löschen eines Kontaktpunkts aus einer Kontaktpunktgruppe

Wenn Sie einen Kontaktpunkt aus einer Kontaktpunktgruppe löschen, wird der Kontaktpunkt nur aus dieser Gruppe entfernt. Wenn Sie einen Kontaktpunkt aus der Gruppe "Alle Kontaktpunkte" löschen, wird der Kontaktpunkt aus der Umgebung und aus Kontaktpunktgruppen, in denen er hinzugefügt wurde, entfernt. Inhaltsadministratoren können einen Kontaktpunkt aus einer Kontaktpunktgruppe löschen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie die Domäne, wählen Sie die zu konfigurierende Umgebung aus, und klicken Sie auf "Sperren".
3. Erweitern Sie die zu konfigurierende Kontaktpunktgruppe.
4. Wählen Sie den Kontaktpunkt aus, der aus der Gruppe entfernt werden soll, und klicken Sie auf "Löschen".
5. Wählen Sie die Umgebung aus, und klicken Sie auf "Entsperren".

   Durch das Dialogfeld "Nicht gespeicherte Daten" werden Sie aufgefordert, die Änderungen zu speichern.
6. Klicken Sie auf "Ja".

Löschen einer Kontaktpunktgruppe

Inhaltsadministratoren können eine anwendererstellte Kontaktpunktgruppe und die entsprechenden Kontaktpunkte aus einer Umgebung löschen. Durch dieses Verfahren wird der Kontaktpunkt aus keiner anderen Gruppe in der Umgebung gelöscht. Sie können die Gruppe "Alle Kontaktpunkte" nicht löschen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Erweitern Sie die Domäne, wählen Sie die zu konfigurierende Umgebung aus, und klicken Sie auf "Sperren".
3. Klicken Sie mit der rechten Maustaste auf die aus der Umgebung zu entfernende Kontaktpunktgruppe, und klicken Sie auf "Löschen".
4. Wählen Sie die Umgebung aus, und klicken Sie auf "Entsperren".

   Durch das Dialogfeld "Nicht gespeicherte Daten" werden Sie aufgefordert, die Änderungen zu speichern.
5. Klicken Sie auf "Ja".

Kapitel 10: Verwalten von Proxy-Kontaktpunkten

Wenn ein Operator auf einen Proxy-Kontaktpunkt abzielt, wird der Operator auf dem Remote-Host ausgeführt, zu dem der Proxy-Kontaktpunkt-Host eine SSH-Verbindung hat. Keine Agentensoftware ist auf dem Remote-Host installiert. Operatoren können auf einem beliebigen Gerät ausgeführt werden, auf dem Windows- oder UNIX-Betriebssystem ausgeführt wird. Durch einen Proxy-Kontaktpunkt wird die Leistung etwas reduziert, aber er ist nützlich, wenn die Agentensoftware auf keinem Zielhost installiert werden kann.

Um einen Proxy-Kontaktpunkt zu verwenden, konfigurieren Sie einen CA Process Automation-Kontaktpunkt, der auf ein Remote-Ziel zeigt, und einen SSH-Anwender auf dem Zielcomputer erstellen.

Dieses Kapitel enthält folgende Themen:

Proxy-Kontaktpunkte – Voraussetzungen

Proxy-Kontaktpunkte können erstellt werden, indem Sie einen vorhandenen Kontaktpunkt so konfigurieren, dass er als Proxy-Kontaktpunkt für einen Remote-Computer oder ein anderes Gerät ausgeführt wird. Ein Kontaktpunkt kann als Proxy-Kontaktpunkt für einen Host mit einer UNIX- oder Windows-Betriebsumgebung konfiguriert werden. Proxy-Kontaktpunkte verwenden SSH, um Aktionen auf Zielcomputern auszuführen.

Die Nutzungsvoraussetzungen für Proxy-Kontaktpunkte sind wie folgt:

- Java Virtual Machine (JVM) Version 1.6+ ist auf dem Host mit dem Kontaktpunkt, der als Proxy-Kontaktpunkt konfiguriert werden soll, erforderlich.
- Wenn das Ziel eines Proxy-Kontaktpunkts ein UNIX-Computer ist, muss die Korn-Shell (ksh) auf dem Zielcomputer installiert werden. Installieren Sie anderenfalls die Korn-Shell, oder verknüpfen Sie sie von der Bash-Shell aus.
- Ein SSH-Anwenderkonto muss auf dem Remote-Computer angegeben werden, auf den ein Proxy-Kontaktpunkt verweist.
- (Optional) Um eine Authentifizierung mit einem öffentlichen Schlüssel zu verwenden, muss eine Vertrauensstellung vom Proxy-Kontaktpunkt-Host zum Ziel-Remote-Computer erstellt werden.

  Wichtig! Wenn Sie diesen Schritt ausführen, müssen Sie den Richtlinien entsprechen, die in den CA Process Automation-spezifischen Anforderungen für SSH-Konnektivität dokumentiert sind.
- In CA Process Automation muss der Proxy-Kontaktpunkt mit Authentifizierungsinformationen und anderen Spezifikationen für den Remote-Host konfiguriert werden.

CA Process Automation-spezifische Anforderungen für SSH-Konnektivität

SSH-Konnektivität kann durch das Erstellen eines SSH-Anwenderkontos auf jedem Zielhost erreicht werden. Wenn Sie die optionale Vertrauensstellung zwischen einem Agentenhost und einem Remote-Host erstellen, gelten bestimmte CA Process Automation-spezifische Konfigurationsvoraussetzungen.

Wenn eine Anfrage an einen Remote-Host verarbeitet wird, werden die folgenden Eigenschaften gelesen:

- Remote-Anwendername.
- Remote-Kennwort.
- SSH-Schlüsselpfad, falls konfiguriert.

CA Process Automation versucht eine SSH-Verbindung vom Agentenhost zum Remote-Host, der in der Anfrage angegeben ist, herzustellen. Der erste Zugangsversuch wird mit den konfigurierten Anmeldeinformationen des Anwenderkontos unternommen. Wenn dieser Versuch fehlschlägt, wird ein zweiter Versuch mithilfe der schlüsselbasierten Authentifizierung unternommen. Um SSH-Authentifizierung mit öffentlichem Schlüssel mit CA Process Automation zu verwenden, muss der Name des privaten Schlüssels mit dem Namen des Anwenderkontos übereinstimmen. Wenn beim Erstellen der Schlüssel eine Passphrase angegeben wird, muss die Passphrase mit dem Kennwort des Anwenderkontos übereinstimmen. Daher haben die folgenden zwei Felder eine doppelte Funktion.

Remote-Anwendername

Ist der Anwendername für das Anwenderkonto, der verwendet wird, wenn die Authentifizierung auf SSH-Anmeldeinformationen basiert.

Ist auch der Name der Schlüsseldatei, in der der private SSH-Schlüssel beim Konfigurieren im Pfad, der als SSH-Schlüsselpfad konfiguriert wird, gespeichert wird.

Remote-Kennwort

Ist das Kennwort für das Anwenderkonto, das verwendet wird, wenn SSH-Anmeldeinformationen für die Authentifizierung verwendet werden.

Ist auch die Passphrase, die verwendet wird, wenn der öffentliche SSH-Schlüssel für die Authentifizierung verwendet wird.

Folgen Sie diesen Richtlinien, wenn Sie eine Vertrauensstellung vom lokalen Host zum Remote-Host erstellen:

- Geben Sie den Namen des Remote-Anwenders für *Anwendername* ein, wenn Sie den folgenden Befehl eingeben:

  ```
  ssh-keygen -t dsa -b 1024 -f Anwendername
  ```

- Geben Sie das Remote-Kennwort als Passphrase ein.

Erstellen des SSH-Anwenderkontos auf dem Remote-Host des Proxy-Kontaktpunkts

Die Proxy-Kontaktpunktkonfiguration gibt den Remote-Anwendernamen und das Remote-Kennwort des SSH-Anwenderkontos an, das verwendet wird, um auf den Remote-Host zuzugreifen. Das SSH-Anwenderkonto muss über Berechtigungen auf Administratorebene verfügen, die erforderlich sind, um CA Process Automation-Operatoren auf dem Zielcomputer auszuführen. Sie sollten das gleiche Anwenderkonto für alle ähnlich konfigurierten Computer definieren, auf die als Remote-Hosts zugegriffen wird. Fügen Sie zum Beispiel das Konto "*Pamuser*" mit dem gleichen Kennwort zu jedem Remote-Host hinzu.

Wenn ein Proxy-Kontaktpunkt eine Verbindung zum Remote-Host initiiert, wird ein temporäres Verzeichnis namens "c2otmp" auf dem Zielcomputer erstellt. Auf einem UNIX-Computer wird dieses Verzeichnis im Verzeichnis "/home" des SSH-Anwenders erstellt.

Erstellen Sie eine SSH-Vertrauensstellung zum Remote-Host.

Wenn Sie die Authentifizierung durch öffentliche Schlüssel für die Verwendung verfügbar machen möchten, erstellen Sie eine Vertrauensstellung vom Proxy-Kontaktpunkt-Host zum Ziel-Remote-Host. Testen Sie dann die SSH-Konnektivität von dem Computer aus, auf dem der Proxy-Kontaktpunkt zum Zielcomputer ausgeführt wird. Eine Vertrauensstellung wird zwischen zwei Hostcomputern erstellt.

CA Process Automation verwendet die Authentifizierung durch öffentliche Schlüssel, die Sie nur dann konfigurieren, wenn die Anwender/Kennwortauthentifizierung fehlschlägt.

Um eine Vertrauensstellung zu erstellen, verwenden Sie das Programm "ssh-keygen", um das Paar aus privatem und öffentlichem Schlüssel zu generieren. Der private Schlüssel bleibt mit dem Agenten auf dem Host. Kopieren Sie den öffentlichen Schlüssel auf den Ziel-Remote-Host, der über keinen Agenten verfügt.

Gehen Sie folgendermaßen vor:

1. Generieren Sie ein Schlüsselpaar. Verwenden Sie den folgenden Befehl, wobei *Anwendername* dem Anwendernamen des SSH-Anwenderkontos entspricht, das Sie auf dem Zielcomputer erstellt haben.

   ```
   ssh-keygen -t dsa -b 1024 -f Anwendername
   ```

   Sie werden aufgefordert, eine Passphrase anzugeben, die später als Kennwort verwendet wird.

2. Geben Sie die Passphase als Antwort auf die Aufforderung an.

   Die private Schlüsseldatei namens *Anwendername* und die öffentliche Schlüsseldatei namens <Anwendername>.werden erstellt.

3. Platzieren Sie die private Schlüsseldatei namens *Anwendername* an einem der folgenden Speicherorte:

   - Das Verzeichnis der privaten Schlüssel, das in der Proxy-Konfiguration angegeben wurde.

     Auf den Schlüssel wird von diesem Verzeichnis aus mit einem Host zugegriffen, für den es keine Datei *Zielhostname*/*Anwendername* gibt.

   - Das Verzeichnis SshKeys/*Zielhostname*, ein Unterverzeichnis des Verzeichnisses mit den privaten Schlüsseln, das in der Proxy-Konfiguration angegeben wird. Auf den privaten Schlüssel wird von diesem Verzeichnis aus zugegriffen, wenn versucht wird, eine Verbindung von *Anwendername* zu *Zielhostname* herzustellen.

     Die Option "SSH-Schlüsselpfad" gibt den Speicherort für das Verzeichnis mit den privaten Schlüsseln im Eigenschaftsdialogfeld "Proxy-Kontaktpunkt" an.

4. Übertragen Sie die Datei des öffentlichen Schlüssels (*Anwendername*.pub) auf den Zielhost, und platzieren Sie sie dort, wo sie vom SSH-Daemon gefunden werden kann.

   Unterschiedliche SSH-Daemons folgen unterschiedlichen Konventionen. Überprüfen Sie die Optionen von "ssh-keygen" auf Details, wie zum Beispiel Formatierungsanforderungen für die Datei des öffentlichen Schlüssels.

5. Für "OpenSsh" muss die öffentliche Datei mit der Datei verkettet werden, die autorisierte Schlüssel für den Anwendernamen enthält. Führen Sie folgenden cat-Befehl auf dem Proxy-Ziel-SSH-Host aus:

   ```
   cat Anwendername.pub >> ~Anwendername/.ssh/authorized_keys
   ```

Weitere Informationen:

CA Process Automation-spezifische Anforderungen für SSH-Konnektivität (siehe Seite 258)

Konfigurieren von Proxy-Kontaktpunkteigenschaften

Sie können einen Proxy-Kontaktpunkt erstellen, indem Sie einen vorhandenen Agentenkontaktpunkt neu konfigurieren, um auf einen angegebenen Remote-Computer zu verweisen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie den Knoten "Domäne", klicken Sie auf die zu konfigurierende Umgebung, und klicken Sie auf Sperren.
3. Wählen Sie unter "Alle Kontaktpunkte" den Agentenkontaktpunkt aus, den Sie als Proxy-Kontaktpunkt festlegen möchten.
4. Stellen Sie sicher, dass die folgenden Eigenschaften festgelegt sind:
   - Automatische Operator-Wiederherstellung
   - Kontaktpunktsicherheit

   Wenn diese Eigenschaften nicht festgelegt sind, lesen Sie Konfigurieren von Kontaktpunkteigenschaften (siehe Seite 238).
5. Aktivieren Sie das Kontrollkästchen Proxy-Kontaktpunkt.

   Die Auswahl zeigt an, dass dieser Kontaktpunkt ein Proxy-Kontaktpunkt ist. Ein Proxy-Kontaktpunkt wird einem Remote-Host zugeordnet. Auf einem Remote-Host sind normalerweise keine Agenten installiert.

6. Konfigurieren Sie den Remote-Host und die Werte für SSH-Authentifizierung. Führen Sie die folgenden Schritte durch:

   a. Geben Sie den absoluten oder relativen Pfad auf dem Agenten-Host, auf dem die Datei des privaten Schlüssels gespeichert ist, im Feld SSH-Schlüsselpfad ein.

      Der Name der privaten Schlüsseldatei, "<Anwendername>", und der Name der öffentlichen Schlüsseldatei, "<Anwendername>.pub", stimmen mit dem Remote-Anwendernamen des Anwenderkontos überein.

   b. Identifizieren Sie den Remote-Host mit seinem vollqualifizierten Domänennamen oder seiner IP-Adresse im Feld Remote-Host.

      Hinweis: Informationen finden Sie im Abschnitt für die Syntax für DNS-Hostnamen (siehe Seite 428).

   c. Geben Sie den Anwendernamen, mit dem eine Verbindung zum SSH-Daemon auf dem Zielhost hergestellt wird, im Feld Remote-Anwendername ein.

      Das SSH-Anwenderkonto muss über ausreichende Berechtigungen für die Durchführung von Administrationsaufgaben auf dem Zielcomputer verfügen.

   d. Geben Sie das Kennwort für das Anwenderkonto ein, das dem Remote-Anwendernamen zugeordnet ist.

      Dieser Wert wird auch als Passphrase verwendet, wenn mithilfe der SSH-Authentifizierung mit öffentlichem Schlüssel Verbindungen hergestellt werden.

   e. Geben Sie die Höchstanzahl von gleichzeitigen Verbindungen, die der Proxy-Kontaktpunkt auf dem Ziel-Remote-Host öffnen kann, im Feld Höchstanzahl aktiver Prozesse ein.

      Eine SSH-Verbindung bleibt geöffnet, während ein Programm oder Skript auf dem Zielhost ausgeführt wird. Wenn Sie diesen Wert auf 20 festlegen und versuchen, 40 Skripte gleichzeitig auf dem Remote-Host auszuführen, werden nur 20 Skripte ausgeführt. Skripts, die nicht gestartet werden, bleiben in der Warteschlange, bis andere abgeschlossen sind. Dann werden sie gestartet.

   f. Wählen Sie das Betriebssystem des Ziel-Remote-Hosts aus.

7. Klicken Sie auf "Speichern".

8. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie Entsperren aus.

Verwenden eines Proxy-Kontaktpunkts

Wenn ein Prozess ausgeführt wird, führen Operatoren im Prozess Betriebsabläufe auf Zielhosts aus. Um einen Operator auf einem Remote-Host ohne Agenten ausgeführt werden, erstellen Sie zunächst eine SSH-Verbindung vom Agentenhost zum Remote-Host. Wenn Sie einen Kontaktpunkt erstellen und einen Agenten mit einer Verbindung zu einem Remote-Host auswählen, wird dieser Kontaktpunkt zu einem Proxy-Kontaktpunkt. Wenn ein Operator einen Proxy-Kontaktpunkt als Ziel angibt, wirkt sich der Betriebsablauf auf den Remote-Host aus.

Um einen Vorgang auf vielen ähnlich konfigurierten Proxy-Kontaktpunkten auszuführen, können Sie die Proxy-Kontaktpunkte in einer Kontaktpunktgruppe gruppieren. Geben Sie dann die Kontaktpunktgruppe als Ziel an, wenn Sie die Operator-Eigenschaften konfigurieren. Zur Laufzeit wird der Operator auf allen Proxy-Kontaktpunkten in der Gruppe ausgeführt.

Weitere Informationen:

Verwalten von Kontaktpunktgruppen (siehe Seite 250)

Kapitel 11: Verwalten von Hostgruppen

CA Process Automation kann Operatoren auf einem Ziel ohne Agenten oder Kontaktpunkt ausführen, wenn Sie in einer Hostgruppe auf dieses Ziel verweisen. Inhaltsdesigner können ein solches Ziel über seine IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) angeben.

Hinweis: Informationen finden Sie im Abschnitt für die Syntax für DNS-Hostnamen (siehe Seite 428).

Wenn sich die gleiche Hostgruppe auf mehreren Agenten befindet, hängt der für die Ausführung des Operators ausgewählte Agent von der Priorität des Agenten ab.

Dieses Kapitel enthält folgende Themen:

Informationen zu Hostgruppen

Eine *Hostgruppe* stellt eine Gruppe von Hosts dar, normalerweise mit ähnlichen Namen oder IP-Adressen, die in einem Operator mit dem FQDN oder der IP-Adresse angegeben werden können. Eine Hostgruppe verweist auf Hosts als Teilnetze von IP-Adressen, Host-Namensmuster oder eine Liste bestimmter IP-Adressen und FQDNs.

Hostgruppen stellen direkten Zugriff bereit, das heißt, die Fähigkeit, eine IP-Adresse oder einen FQDN in einem Operator anzugeben, im Gegensatz zu einem Kontaktpunkt- oder Proxy-Kontaktpunktnamen. Hosts, auf die in einer Hostgruppe verwiesen wird, benötigen keine Agenten- oder Proxy-Kontaktpunkt-Zuordnungen. Vermeiden Sie das Einschließlich eines Hosts, der zu einem geclusterten Koordinationsrechner in einer Hostgruppe gehört. Inhaltsdesigner können nicht durch seine IP-Adresse oder seinen FQDN auf einen solchen Host verweisen.

Sie können mehreren Hostgruppen auf dem gleichen Agenten definieren. Ein bestimmter Agent könnte eine Hostgruppe für Varianten eines Windows-Betriebssystems und eine weitere Hostgruppe für Varianten eines UNIX-Betriebssystems haben.

Sie können die gleiche Hostgruppe auf einem oder mehreren Agenten definieren. Wenn sich die gleiche Hostgruppe auf mehreren Agenten befindet, hängt der für die Ausführung des Operators ausgewählte Agent von der Priorität des Agenten ab.

Um CA Process Automation-Operatoren auf einem Remote-Host auszuführen, muss ein lokaler Host mit einem CA Process Automation-Agenten, der einer Hostgruppe zugeordnet ist, Zugriff auf den Zielhost erhalten. Der Agent verwendet SSH, um Zugriff auf einen Ziel-Remote-Host zu erhalten und Operatoren darauf auszuführen. Sie definieren den SSH-Zugriff vom Agentenhost zu jedem von der Hostgruppe mit einem SSH-Anwenderkonto dargestellten Zielhost und optional eine vertrauenswürdige SSH-Beziehung.

Eigenschaften für eine Hostgruppe enthalten eine Einstellung für die Höchstanzahl der SSH-Verbindungen. SSHD-Server weisen normalerweise in Standardkonfigurationen Limits auf. Die SSH-Verbindung bleibt geöffnet, während das Programm oder Skript auf dem Zielhost ausgeführt wird. CA Process Automation implementiert interne Warteschlangen pro Ziel. Wenn Sie den Wert auf 20 festlegen und Sie dann auf dem Zielhost 40 Skripte gleichzeitig ausführen, werden nur 20 Skripte gleichzeitig ausgeführt. Neue Skripte werden gestartet, wenn die Ausführung anderer Skripte beendet ist. Bei Hostgruppen, bei denen ein- und derselbe Agent für mehrere Remote-Hosts als Proxy fungiert, verfügt jeder Remote-Host über ein spezifisches Limit. Daher wirkt sich diese Einstellung nicht auf die Anzahl der Hosts in der Hostgruppe aus. Das Limit für die Anzahl von Hosts ist die Höchstanzahl von gleichzeitigen TCP-Verbindungen, die das Betriebssystem für den Agenten unterstützt. Bestimmte Betriebssysteme unterstützen eine hohe Anzahl von gleichzeitigen TCP-Verbindungen.

Wichtig! Obwohl eine Hostgruppe Remote-Hosts mit Agenten einschließen kann, erstellen Sie keine Hostgruppe aus Hosts mit Agenten, um direkt auf sie verweisen zu können. Der Verweis über Kontaktpunkt und Proxy-Kontaktpunkt sollte aus Gründen der Flexibilität und Verarbeitungsgeschwindigkeit bevorzugt werden.

Hostgruppen-Implementierungsprozess

Sie können auf jedem vorhandenen Agenten eine Hostgruppe konfigurieren. Ein Agent muss nicht als Kontaktpunkt konfiguriert werden, um eine Hostgruppe hosten zu können. Der Agentenhost für die Hostgruppe verwendet SSH, um auf Aktionen auf einem Remote-Host zuzugreifen und sie auszuführen. Ein Bestandteil der Hostgruppen-Vorbereitung ist die Aktivierung der SSH-Authentifizierung. Wenn Inhaltsdesigner ein Mitglied einer Hostgruppe in einer Operatordefinition als Ziel festlegen, referenzieren sie den Zielhost anhand seiner IP-Adresse oder seines vollqualifizierten Domänennamens (FQDN).

Bereiten Sie die Verwendung einer Hostgruppe vor, indem Sie die folgenden Aufgaben und Verfahren durchführen. Auf diese Prozessübersicht folgen Themen, die Einzelheiten zu den jeweiligen Verfahren bieten.

1. Erstellen Sie eine Hostgruppe. (siehe Seite 269)
2. Konfigurieren Sie die Eigenschaften der Hostgruppe (siehe Seite 270). d. h. geben Sie Werte für alle Einstellungen mit Ausnahme von "SSH-Schlüsselpfad" an.
   - Informationen zur Eingabe von Mustern finden Sie unter Definieren von Mustern für Remote-Hostnamen mit regulären Ausdrücken (siehe Seite 271).
   - (Optional) Bei einer Authentifizierung mit öffentlichem Schlüssel konfigurieren Sie "SSH-Schlüsselpfad".

     Hinweis: CA Process Automation erhält nur mit der Authentifizierung mit öffentlichem Schlüssel Zugriff, wenn der Zugriff mit den Anmeldeinformationen des Anwenderkontos fehlschlägt.
3. Überprüfen Sie im Agenten-Host für die Hostgruppe, dass Version 1.7 oder 1.6 von Java Virtual Machine (JVM) (höchstens Version 1.6.0_45) installiert ist. Im Lieferumfang von JVM ist JRE oder JDK enthalten. Für Agenten, die auf Hosts mit Windows-Betriebssystemen installiert sind, wird sowohl 32-Bit- als auch 64-Bit-JVM unterstützt. Verwenden Sie folgenden Befehl, um sicherzustellen, dass Ihre Java-Version eine gültige Version ist. Es folgt ein Beispiel:

   ```
   java -version
   ```

   Beispielantwort:

   ```
   Java-Version "1.6.0_x" ist eine gültige Version
   ```
4. Erstellen von SSH-Anmeldeinformationen auf Hosts in einer Hostgruppe (siehe Seite 274). Definieren Sie ein Anwenderkonto mit den SSH-Anmeldeinformationen, die in den Hostgruppeneigenschaften für "Remote-Anwendername" und "Remote-Kennwort" angegeben werden.
5. Überprüfen Sie auf jedem UNIX-Remote-Host, der von der Hostgruppe referenziert wird, ob die Korn-Shell installiert ist. Wenn die Korn-Shell nicht installiert ist, führen Sie eine der folgenden Aktionen aus:
   - Installieren Sie die Korn-Shell.

- Erstellen Sie einen Softlink von einer vorhandenen Bash-Shell zur Korn-Shell mithilfe des zurückgegebenen Speicherorts. Zum Beispiel:

```
ln –s  /bin/bash /bin/ksh
```

6. Führen Sie die folgenden Schritte aus, um die Konfiguration der Authentifizierung mit öffentlichem Schlüssel abzuschließen. Diese Schritte beziehen sich auf die Spezifikationen in "SSH-Schlüsselpfad".

   - Stellen Sie sicher, dass der Pfad, den Sie in der Hostgruppenkonfiguration für "SSH-Schlüsselpfad" eingegeben haben, auf dem Agentenhost vorhanden ist. Andernfalls erstellen Sie ihn. Zum Beispiel:

     Windows: C:\PAM\Sshkeys

     UNIX: /home/PAM/Sshkeys

   - Stellen Sie sicher, dass Sie über das Hilfsprogramm ssh-keygen verfügen. Andernfalls laden Sie es herunter. Auf einem Windows-System wird die Datei "ssh-keygen.exe" im Verzeichnis "C:\Programme\OpenSSH\bin" angezeigt. Das Verzeichnis "bin" enthält zudem weitere Dateien, die es Ihnen ermöglichen, UNIX-Befehle zu verwenden.

     Sie verwenden dieses Hilfsprogramm, um das private/öffentliche Schlüsselpaar zu generieren.

   - Stellen Sie sicher, dass Sie eine Datei von einem Host auf einen anderen kopieren können. Laden Sie bei Bedarf ein Kopierprogramm wie scp oder Winscp herunter.

     Sie kopieren den öffentlichen Schlüssel vom Agentenhost auf jeden Remote-Host.

   - Erstellen Sie das Zielverzeichnis und die Zieldatei für den öffentlichen Schlüssel (siehe Seite 275).

   - Erstellen einer Vertrauensstellung zu einem Remote-Host, auf den von einer Hostgruppe verwiesen wird (siehe Seite 276).

     Wichtig! Befolgen Sie diese Anweisungen sorgfältig. Die Schritte umfassen spezifische Anforderungen für CA Process Automation, die sich von der Standardimplementierung von DSA-Schlüsselpaaren unterscheiden.

Weitere Informationen:

CA Process Automation-spezifische Anforderungen für SSH-Konnektivität (siehe Seite 258)

Erstellen einer Hostgruppe

Sie können eine Hostgruppe zu einer ausgewählten Umgebung hinzufügen und dann den Agenten auswählen. Sie können auch eine Hostgruppe auf einem Agenten konfigurieren und dann die Umgebung auswählen. Die Kombination aus Agentennamen und Hostgruppennamen muss innerhalb einer Umgebung eindeutig sein.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Wählen Sie die Umgebung aus, die konfiguriert werden soll, und klicken Sie auf Sperren.
3. Um eine Hostgruppe zu einer ausgewählten Umgebung hinzuzufügen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie mit der rechten Maustaste auf die gesperrte Umgebung, und wählen Sie Hostgruppe hinzufügen aus.

      Hostgruppe hinzufügen: *Umgebung* wird angezeigt.
   b. Geben Sie den Hostgruppennamen ein.
   c. Wählen Sie einen angezeigten Agenten aus, und klicken Sie auf Hinzufügen.
4. Um eine Hostgruppe zu einem ausgewählten Agenten hinzuzufügen, führen Sie die folgenden Schritte aus:
   a. Erweitern Sie den Knoten "Agenten".
   b. Klicken Sie mit der rechten Maustaste auf den gewünschten Agenten, wählen Sie Hostgruppe konfigurieren in aus, und wählen Sie die gewünschte Umgebung aus.

      Das Dialogfeld Agenten-Hostgruppe hinzufügen wird eingeblendet.
   c. Geben Sie den Hostgruppennamen ins Feld Hostgruppenname ein, und klicken Sie auf OK.

      Wenn Sie den Namen einer vorhandenen Hostgruppe eingeben, wird der ausgewählte Agent dieser vorhandenen Hostgruppe zugeordnet.
5. Zeigen Sie den Hostgruppennamen folgendermaßen an:
   - Erweitern Sie den Knoten Alle Hostgruppen für die Umgebung, in der Sie die Hostgruppe erstellt haben.
   - Erweiter Sie "Agenten", und wählen Sie den Agenten mit der Hostgruppe aus. Die neue Hostgruppe wird auf der Registerkarte Verbundene Kontaktpunkte und Hostgruppen mit dem Pfad der Domänenhierarchie aufgelistet.

Weitere Informationen:

Hostgruppen-Implementierungsprozess (siehe Seite 267)

Konfigurieren von Hostgruppeneigenschaften

Sie können Eigenschaften einer Hostgruppe innerhalb der Registerkarte "Konfiguration" konfigurieren. Sie stellen die Konnektivität zwischen dem Agenten und jeden Remote-Host in der Hostgruppe mit Produkten von Drittanbietern her.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie die Domäne.
3. Erweitern Sie die Umgebung mit der Hostgruppe.
4. Erweitern Sie alle Hostgruppen.
5. Wählen Sie die zu konfigurierende Hostgruppe aus, und klicken Sie dann auf die Registerkarte "Eigenschaften".
6. Legen Sie die Eigenschaften der ausgewählten Hostgruppe fest.
   a. Legen Sie bei Bedarf "Automatische Operator-Wiederherstellung" und "Kontaktpunktsicherheit" fest, oder akzeptieren Sie den Standard "Von Umgebung erben".
   b. Geben Sie für "SSH-Schlüsselpfad" den Zielpfad an, den Sie auf dem Agenten für das Speichern der privaten Schlüsseldatei erstellt haben.

      Wenn der Agentenhost über ein Windows-Betriebssystem verfügt, geben Sir Folgendes ein:
      `C:\PAM\SshKeys`

      Wenn der Agentenhost über ein UNIX- oder Linux-Betriebssystem verfügt, geben Sie Folgendes ein:
      `/home/PAM/Sshkeys`

      Wichtig! Erstellen Sie den Zielpfad auf dem Agentenhost.
   c. Klicken Sie für jedes Remote-Host-Namensmuster auf die Schaltfläche "Parameter hinzufügen", und definieren Sie ein Host-Namensmuster.

      Weitere Informationen finden Sie unter "Definieren von Namensmustern für den Remote-Host mithilfe von regulären Ausdrücken (siehe Seite 271)".
   d. Geben Sie die Anmeldeinformationen des Anwenderkontos ein, das Sie auf einem Remote-Host, der von dieser Hostgruppe referenziert ist, erstellt haben oder erstellen wollten.

      Hinweis: Wenn Sie die Authentifizierung mit öffentlichem Schlüssel konfigurieren, muss dieser Wert in dem Befehl zum Generieren von Schlüsseldateien als *Anwendername* angegeben werden. Wenn Sie eine öffentliche Schlüsselauthentifizierung mit einer Passphrase verwenden, geben Sie die Passphrase für "Remote-Kennwort" ein.
   e. Füllen Sie die verbleibenden intuitiven Felder aus.

7. Klicken Sie auf "Speichern".
8. Klicken Sie mit der rechten Maustaste auf die gesperrte Umgebung, und wählen Sie Entsperren aus.

   Das Konfigurieren der Eigenschaften ist Teil der gesamten Konfiguration. Sie müssen ein Anwenderkonto auf jedem Remote-Host mit den hier konfigurierten Anmeldeinformationen erstellen. Dadurch wird der SSH-Zugriff vom Agenten zu jedem Remote-Host in der Hostgruppe bereitgestellt. Das Einrichten einer Beziehung mit öffentlichen und privaten Schlüsseln ist optional.

Weitere Informationen:

Hostgruppen-Implementierungsprozess (siehe Seite 267)

Definieren von Namensmustern für den Remote-Host mithilfe von regulären Ausdrücken:

Wenn Sie Hostgruppen konfigurieren, geben Sie Host-Namensmuster und IP-Adressmuster oder beide an. Reguläre Ausdrucks-Operatoren, die Sie anwenden können, wenn Remote-Hostmuster für Hostgruppen definieren, folgen diesem Format:

- ^ (Caret) bedeutet "startet mit".
- \ (Escape) bedeutet die Interpretation des folgenden Operator-Zeichens als wörtliche Zeichenfolge.
- . (Punkt) innerhalb eines Ausdrucks bedeutet ein beliebiges Zeichen. Der Ausdruck "a.b" stimmt mit jeder Zeichenfolge überein, die aus drei Zeichen besteht und mit "a" beginnt und mit "b" endet.
- .* (Punktsternchen) bedeutet, dass ein beliebiges Zeichen beliebig oft akzeptiert wird. Der Ausdruck "a.*b" entspricht einer Zeichenfolge beliebiger Länge, die mit "a" beginnt und mit "b" endet.
- $ (Dollarzeichen) bedeutet "endet mit".

Stellen Sie sich den regulären Ausdruck als Möglichkeit vor, alles im FQDN auszudrücken, einschließlich:

- ein Anfangsmuster (^String)
- ein Mittelmuster (String)
- ein Endmuster (String$)
- ein genaues Muster (^StringWithEscapedDots$)

Die folgende Tabelle enthält Beispiele, die entworfen wurden, um Ihnen dabei zu helfen, Namensmuster für Hosts in eine Weise einzugeben, die die effiziente Verarbeitung sicherstellt. Wenn Sie einen FQDN oder eine Unterdomäne ohne Operatoren eingeben, wird der FQDN oder die Gruppe, den bzw. die Sie zuzuordnen möchten, gefunden, aber die Verarbeitung ist weniger effizient. Es hat sich bewährt, die folgenden Kombinationen aus regulären Ausdrücken in die Namensmuster für Hosts, die Sie für Remote-Host-Muster eingeben, einzuschließen.

Übliche Kombinationen	Beschreibung	Beispielhafter FQDN und beispielhafte Hostgruppe
^<Hostname>	Das Caret-Zeichen als erstes Zeichen bedeutet, dass das Muster mit dem Text beginnt, der dem Caret-Zeichen folgt.	**FQDN:** "^host1\.ca\.com$" stimmt nur mit "host1.ca.com" überein. (Aber "host1\.ca\.com$" ohne das vorstehende Caret-Zeichen sucht nach jedem Host mit einem Namen, der mit "host1.ca.com, wie aaaahost1.ca.com" endet) **Gruppe:** "ca\.com$" ohne das vorstehende Caret-Zeichen entspricht jedem FQDN in der Unterdomäne "ca.com".
\.	Die Escape-Punkt-Kombination (\.) bedeutet, dass der Punkt als Literalzeichen interpretiert wird.	**FQDN:** "^host1\.ca\.com$" stimmt nur mit "host1.ca.com" überein. (Aber "^host.ca.com$" ohne Escape-Zeichen vor dem Punkt kann Folgendem entsprechen: host1Mca0com) **Gruppe:** "^host.\.ca\.com$" mit einem Punkt nach "host" kann Hosts mit dem Namen {host0, host1, ...hostZ} in der Domäne "ca.com" entsprechen.
.*<Domäne>	Die Punktsternchenkombination (.*) ermöglicht eine volle Übereinstimmung.	**Gruppe:** ".*\.ca\.com$", eine durch ".*" eingeleitete Domäne, entspricht allen Hosts in der Domäne.
<Domänenname>$	Das Dollarzeichen nach einem Domänennamen bedeutet, dass das Muster mit der angegebenen Domäne endet.	**FQDN:** "^host1\.ca\.com$" stimmt nur mit "host1.ca.com" überein. (Aber "^host1\.ca\.com" ohne den abschließenden $-Operator kann Folgendem entsprechen: "host1.ca.comaaaaaaa")

Beispiele

Muster für Remote-IP-Adresse

Gibt eine Kombination der folgenden Elemente an, in denen IP-Adressen eher statisch als dynamisch sind. Klicken Sie auf "Hinzufügen", um jede Zeile zu erstellen.

- eine Liste von IPv4-IP-Adressen
- ein oder mehrere IPv4-Subnetze mit CIDR-Notation

Namensmuster für Remote-Host

Gibt eine Gruppe von Remote-Hosts mit einer Liste von vollqualifizierten Domänennamen (FQDN) oder reguläre Ausdrücke für eine Unterdomäne an. Wählen Sie "Hinzufügen", um eine Zeile für jede Mustereingabe zu erstellen.

Zum Beispiel:

- abc\.mycompany\.com
- .*pam-lnx\.mycompany\.com$

  Dieses Muster stimmt mit jedem Hostnamen in Ihrer Unternehmensdomäne überein, der auf "pam-lnx" endet, wobei "mycompany" durch den Namen Ihres Unternehmens ersetzt wird.

- ^machine1\.mycompany\.com$

  Konkret drückt "^machine1\.mycompany\.com$" einen vollqualifizierten Domänennamen (FQDN) als regulären Ausdruck aus. Dieses Muster stimmt nur mit dem FQDN überein, der diesen Kriterien entspricht:

  Beginnt mit *machine1.*

  Endet mit *com.*

  Enthält *machine1*, dann einen *Punkt*, dann *mycompany*, dann einen *Punkt* und dann *com*.

Erstellen von SSH-Anmeldeinformationen auf Hosts in einer Hostgruppe.

Eine Hostgruppenkonfiguration gibt die SSH-Anmeldeinformationen folgendermaßen an.

- Remote-Anwendername
- Remote-Kennwort

Melden Sie sich bei jedem Host an, den die Hostgruppen referenziert. Erstellen Sie ein Anwenderkonto mit diesen SSH-Anmeldeinformationen. Dieses SSH-Anwenderkonto muss über ausreichende Berechtigungen für folgende Aufgaben verfügen:

- Um administrative Aufgaben auszuführen.
- Um CA Process Automation-Operatoren auf jedem Zielcomputer auszuführen.

Der Agent verwendet den Anwendernamen des SSH-Anwenderkontos, um eine Verbindung zum SSH-Daemon auf dem Ziel-Remote-Host herzustellen. Der Zielhost kann ein Host sein, der den Namensmustern für Remote-Hosts oder den Remote-IP-Adressmustern in der Hostgruppenkonfiguration entspricht.

Der Agentenhost der Hostgruppe initiiert folgendermaßen eine Verbindung zum Remote-Host:

1. Beim Remote-Host wird eine Anmeldung mit den angegebenen Anmeldeinformationen durchgeführt.
2. Es wird ein temporäres Verzeichnis mit dem Namen "c2otmp" erstellt.

   Dieses Verzeichnis wird im Verzeichnis "/home" des SSH-Anwenders erstellt, wenn der Zielhost ein UNIX-Computer ist. Beispiel:

   ```
   /home/<user_name>/c20tmp
   ```

Weitere Informationen:

Hostgruppen-Implementierungsprozess (siehe Seite 267)

Erstellen Sie das Zielverzeichnis und die Datei für den öffentlichen Schlüssel.

Wenn Sie beschließen, die optionale Vertrauensstellung zu Remote-Hosts, auf die von der Hostgruppe verwiesen wird, zu erstellen, überprüfen Sie zuerst, ob das folgende Verzeichnis und die folgende Datei auf jedem Remote-Host vorhanden sind. Ist das Verzeichnis oder die Datei nicht vorhanden, dann erstellen Sie es bzw. sie.

Folgendes ist auf jedem Remote-Host erforderlich, bevor Sie die Vertrauensstellung zwischen Host und Hostgruppe erstellen können.

- Das .ssh-Verzeichnis unter /home/<Anwendername>, das Zielverzeichnis für <Anwendername>.pub
- Eine authorized_keys-Datei, an die der in <Anwendername>.pub enthaltene öffentliche Schlüssel angehängt werden kann. Die Datei ~/.ssh/authorized_keys ist die Standarddatei, die die für die DSA-Authentifizierung zulässigen öffentlichen Schlüssel enthält.

Sie können das .ssh-Verzeichnis und die authorized_keys-Datei auf einem UNIX- oder Linux-Remote-Host erstellen.

Gehen Sie folgendermaßen vor:

1. Verwenden Sie ssh, um auf einen Remote-Host zuzugreifen, und melden Sie sich mit dem für die Hostgruppe konfigurierten Remote-Anwendernamen und Remote-Kennwort an.
2. Stellen Sie sicher, dass das aktuelle Verzeichnis Ihr Stammverzeichnis ist. Geben Sie ein:

   pwd

   Die Antwort lautet:

   `/home/`*`Anwendername`*
3. Erstellen Sie das. ssh-Verzeichnis in diesem Pfad, und wechseln Sie zum neuen Verzeichnis.

   ```
   mkdir .ssh
   cd .ssh
   ```
4. Erstellen Sie die Datei authorized_keys im. ssh-Verzeichnis.

   ```
   cat > authorized_keys
   ```

   Eine leere authorized_keys-Datei wird im Verzeichnis "/home/*Anwendername*/.ssh" erstellt.

So erstellen das .ssh-Verzeichnis und die authorized_keys-Datei auf einem-Remote-Host mit Windows

1. Greifen Sie über Remote-Desktop auf den Remote-Host zu, und melden Sie sich mit dem für die Hostgruppe konfigurierten Remote-Anwendernamen und Remote-Kennwort an.

2. Navigieren Sie zu Ihrem Stammordner. Zum Beispiel \Users*Anwendername.*
3. Wenn kein Ordner namens .ssh vorhanden ist, erstellen Sie einen neuen Ordner und nennen ihn .ssh.
4. Erstellen Sie im folgenden Ordner eine Datei mit dem Namen authorized_keys ohne Dateinamenerweiterung.

   `\Users\Anwendername\.ssh`

   Die folgende leere Datei wird erstellt.

   `\Users\Anwendername\.ssh\authorized_keys`

Erstellen einer Vertrauensstellung zu einem Remote-Host, auf den von einer Hostgruppe verwiesen wird

Ein *Remote-Host* ist ein Host, den eine Hostgruppe referenziert. Die Hostgruppe wird auf einem Host mit einem Agenten konfiguriert. Der Remote-Host hat normalerweise keinen Agenten. Um einen Remote-Host als Ziel festzulegen, ist es erforderlich, dass ein Prozessoperator eine SSH-Konnektivität zwischen einem Agentenhost und dem referenzierten Remote-Host hat.

Stellen Sie eine SSH-Verbindung mit einer der folgenden Methoden her:

- Stellen Sie eine Vertrauensstellung zwischen dem Agenten-Host und dem Remote-Host her. Diese Methode erstellt ein Paar aus öffentlichen/privaten Schlüsseln.
- Erstellen Sie ein Anwenderkonto auf dem Remote-Host. Diese Methode erstellt Anmeldeinformationen.

Wenn Sie ein Anwenderkonto *und* eine Vertrauensstellung erstellen, verwendet das Produkt die Vertrauensstellung als Backup-Mechanismus. Wenn die Authentifizierung für die konfigurierten Anmeldeinformationen fehlschlägt, dann verwendet das Produkt das Schlüsselpaar zur Authentifizierung.

Generieren Sie ein Schlüsselpaar mit dem Programm "SSH-keygen". Speichern Sie den privaten Schlüssel in den konfigurierten SSH-Schlüsselpfad, und kopieren Sie dann den öffentlichen Schlüssel in die Remote-Hosts, die von der Hostgruppe referenziert werden. Platzieren Sie den öffentlichen Schlüssel dort, wo sie der SSH-Daemon finden kann. Der OpenSSH-Daemon "sshd" sucht den Schlüssel in "/home/*Anwendername*/.ssh/authorized_keys".

Sie können eine Vertrauensstellung zu einem Remote-Host erstellen, auf den von einer Hostgruppe verwiesen wird.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Host mit dem Agenten an, auf dem die Hostgruppe definiert wird.

2. Öffnen Sie eine Eingabeaufforderung, und wechseln Sie das Verzeichnis zu dem Pfad, in dem Sie das Schlüsselpaar generieren möchten.

   Wenn Sie zum Beispiel "OpenSSH" auf ein Windows-Betriebssystem heruntergeladen haben, wechseln Sie in das Verzeichnis "C:\Programme\OpenSSH\bin" mit dem Programm "ssh-keygen".

3. Generieren Sie ein Schlüsselpaar mit folgendem Befehl:

   `ssh-keygen -t dsa -b 1024 -f` *`Anwendername`*

   Benutzername

   Gibt den Wert an, den Sie als Remote-Anwendername in der Hostgruppe konfiguriert haben.

   Die folgende Meldung und Aufforderung werden angezeigt:

   `Erstellen des Schlüsselpaares "öffentlich/privat".`

   `Passphrase eingeben <leer für keine Passphrase>:`

4. Geben Sie den Wert ein, den Sie als Remote-Kennwort in der Hostgruppe konfiguriert haben. This value is required. (Dieser Wert ist erforderlich)

   Folgende Eingabeaufforderung wird angezeigt:

   `Geben Sie die gleiche Passphrase erneut ein:`

5. Geben Sie den Wert für das Remote-Kennwort erneut ein.

   Folgende Meldungen werden angezeigt:

   `Ihre Identifikation wurde in` *`Anwendername`* `gespeichert.`

   `Ihre Datei des öffentlichen Schlüssels wurde in` *`Anwendername`*`.pub gespeichert.`

   `Der Schlüsselfingerabdruck ist:`

   `fingerprint_string login_name@host_name`

   Das Produkt erstellt eine private Schlüsseldatei mit dem Namen "*user_name*" und die öffentliche Schlüsseldatei mit dem Namen "*user_name*.pub". Die Passphrase für die Schlüsseldatei ist die gleiche wie das Kennwort des für den SSH-Zugriff verwendeten Anwenderkontos.

6. Verschieben Sie die Datei des privaten Schlüssels namens *Anwendername* in den Speicherort, den Sie als SSH-Schlüsselpfad in der Hostgruppe konfiguriert haben. Zum Beispiel:

   - **Windows:** C:\PAM\Sshkeys
   - **UNIX:** /home/PAM/Sshkeys

7. Übertragen Sie die Datei des öffentlichen Schlüssels *(Anwendername*.pub) auf jeden Host, auf den von der Hostgruppe verwiesen wird, und platzieren Sie sie dort, wo sie der SSH-Daemon finden kann.

   Unterschiedliche SSH-Daemons folgen unterschiedlichen Konventionen. Prüfen Sie die Optionen von "ssh-keygen" auf Informationen, wie z. B. für Formatierungsanforderungen für die Datei des öffentlichen Schlüssels.

8. Hängen Sie für OpenSSH den in "*Anwendername*.pub" enthaltenen öffentlichen Schlüssel an die Datei an, die alle autorisierten, von diesem Host verwendeten Schlüssel enthält. Der OpenSSH-SSH-Daemon (sshd) durchsucht die Datei "authorized_keys". Die Datei "authorized_keys" muss sich im Verzeichnis ".ssh" im Stammverzeichnispfad befinden.

   a. Führen Sie folgenden Befehl auf jedem Host aus, auf den von der Hostgruppe verwiesen wird:

      ```
      cat Anwendername.pub >>
      home/Anwendername/.ssh/authorized_keys
      ```

   b. Wechseln Sie zum Anwender "root", und starten Sie folgenden ssh-Dienst neu:

      ```
      su root
      ```

      ```
      service sshd restart
      ```

9. Überprüfen Sie, ob der Zugriff besteht. Melden Sie sich am Host mit dem Agenten und mit ssh zu am Remote-Host an. Wenn die Anmeldung erfolgreich ist, wird die Vertrauensstellung hergestellt. Geben Sie den folgenden Befehl am Agentenhost ein:

   ```
   ssh Anwendername@Remote-Host
   ```

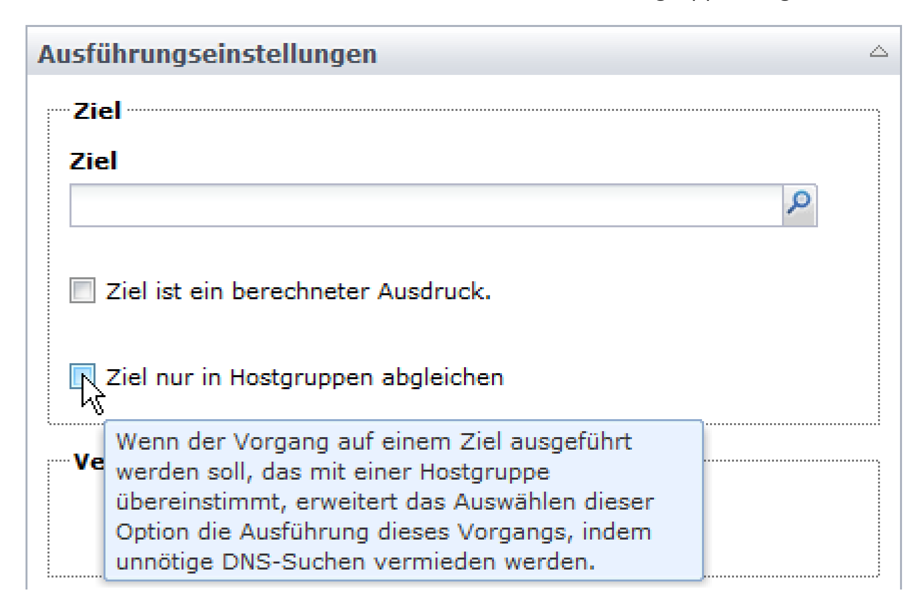
Weitere Informationen:

Hostgruppen-Implementierungsprozess (siehe Seite 267)
CA Process Automation-spezifische Anforderungen für SSH-Konnektivität (siehe Seite 258)

Sicherstellen einer effizienten Verarbeitung von Hostgruppen-Referenzen

Dieses Thema ist für Inhaltsdesigner relevant. Für Administratoren dient es nur Informationszwecken.

Beim Entwerfen von Prozessen legen Inhaltsdesigner Ausführungseinstellungen für die einzelnen Operatoren fest. Das folgende Beispiel ist ein Ausschnitt eines Dialogfelds mit dem Feld "Ziel" und dem Kontrollkästchen "Ziel nur in Hostgruppen abgleichen".



Wenn das Feld Ziel einen Kontaktpunktnamen, einen Proxy-Kontaktpunktnamen oder eine Agenten-ID enthält, deaktivieren Sie das Kontrollkästchen Ziel nur in Hostgruppen abgleichen.

Wenn das Feld Ziel eine IP-Adresse eines bestimmten Hosts enthält, aktivieren das Kontrollkästchen Ziel nur in Hostgruppen abgleichen. Angaben von IP-Adressen oder Hostnamen im Feld Ziel sind nur gültig, wenn eine Hostgruppe in der aktuellen Umgebung den entsprechenden Host referenziert.

Wichtig! Wenn ein Prozess in einem Ordner als vordefinierter Inhalt exportiert werden soll, geben Sie im Feld Ziel keine IP-Adresse ein. Geben Sie stattdessen einen Datensatznamen ein, der die IP-Adresse enthält. Beachten Sie auch:

- Aktivieren Sie Ziel ist ein berechneter Ausdruck.
- Aktivieren Sie Ziel nur in Hostgruppen abgleichen. Ein Datensatz, der eine IP-Adresse referenziert, ist gültig, wenn eine Hostgruppe in der aktuellen Umgebung auf den entsprechenden Host verweist.

Der folgende Beispielfall veranschaulicht den Zweck dieses Kontrollkästchens:

- Das Feld Ziel enthält die Eingabe *Host*, wobei die Eingabe dem Hostnamen eines Hosts in einer Hostgruppe entspricht.
- Das Kontrollkästchen Ziel nur in Hostgruppen abgleichen ist deaktiviert.

Die Laufzeitverarbeitung wertet die Eingabe für Ziel aus und verarbeitet sie in der folgenden Reihenfolge:

1. Wenn die Eingabe ein Kontaktpunktname ist, findet die Ausführung auf dem Host mit dem Agenten statt, der zum Kontaktpunkt zugeordnet ist.
2. Wenn die Eingabe ein Proxy-Kontaktpunktname ist, findet die Ausführung auf dem Host mit der SSH-Verbindung zum Agenten, der dem Kontaktpunkt zugeordnet ist, statt.
3. Wenn die Eingabe eine Agenten-ID ist, findet die Ausführung auf dem Host mit dieser Agenten-ID statt.
4. Wenn die Eingabe eine IP-Adresse oder ein Hostname ist, die bzw. der von einer Hostgruppe referenziert wird, findet die Ausführung auf diesem Host statt.

   Hinweis: Der Operator schlägt fehl, wenn Sie das Kontrollkästchen Ziel nur in Hostgruppen abgleichen auswählen und das angegebene Ziel *nicht* Teil einer Hostgruppe ist. Der Operator schlägt auch dann fehl, wenn das Ziel ein gültiger Kontaktpunktname, ein gültiger Proxy-Kontaktpunktname oder eine gültige Agenten-ID ist.

Fälle, in denen das Verwenden von Hostgruppen-Referenzen vermieden werden soll

Wenn ein Prozess in einem Ordner als vordefinierter Inhalt exportiert wird:

- Prozesse können in der Importumgebung *nicht* geändert werden.
- Datensätze *können* in der Importumgebung geändert werden.

Wenn das Feld "Ziel" eines Operators eine IP-Adresse oder einen Hostnamen enthält, kann der importierte Prozess nicht erfolgreich ausgeführt werden. Die Eingabe für "Ziel" für den Operator kann in der Importumgebung nicht geändert werden.

Für Inhalte, die weiter verwendet werden sollen, wird empfohlen, für die Konfigurationsparameter Datensätze zu verwenden. Der Inhaltsdesigner erstellt eine Datensatzvariable, in der eine IP-Adresse gespeichert ist. Danach gibt der Inhaltsdesigner diese Datensatzvariable im Feld "Ziel" für den Operator ein. Administratoren in der Importumgebung können den Datensatz mit einem IP-Adresswert, der eine Hostgruppe in der Importumgebung referenziert, aktualisieren.

Wie Hostgruppen und Proxy-Kontaktpunkte sich unterscheiden

Hostgruppen und Proxy-Kontaktpunkte sind hinsichtlich der folgenden Punkte identisch:

- Beide werden auf Agenten ausgeführt.
- Beide greifen über SSH auf Remote-Hosts zu.
- Beide unterstützen die gleichen CA Process Automation-Operatoren, die auf Remote-Hosts über SSH ausgeführt werden können.
- Die konfigurierten Kategorien für die erforderlichen Operatoren müssen auf dem Agentenhost ausgeführt werden, auf dem der Proxy-Kontaktpunkt oder Hostgruppe konfiguriert ist.

Hostgruppen unterscheiden sich von Proxy-Kontaktpunkten auf folgende Weise:

- Die Beziehung zwischen einer Hostgruppe und potenziellen Zielhosts ist eins zu viele, während die Beziehung zwischen einem Proxy-Kontaktpunkt und dem Zielhost eins zu eins ist.
- Inhaltsdesigner können auf mehrere Hosts mit zugeordneten Proxy-Kontaktpunkten durch das Angeben einer Kontaktpunktgruppe verweisen. Inhaltsdesigner können nicht auf mehrere Hosts verweisen, die nur eine Hostgruppen-Referenz haben.
- Inhaltsdesigner geben einen Remote-Host als Ziel durch seinen Kontaktpunktnamen an, wenn der Remote-Host einen zugeordneten Proxy-Kontaktpunkt hat. Inhaltsdesigner geben einen Remote-Host als ein Ziel durch seine IP-Adresse oder seinen FQDN an, wenn der Remote-Host eine Hostgruppenreferenz hat.

Kapitel 12: Verwalten von Operatorkategorien und anwenderspezifischen Operatorgruppen

In diesem Kapitel werden Begriffe und Vorgänge beschrieben, die für das Konfigurieren gemeinsamer Standardeinstellungen für Operatoren auf Kategorienebene relevant sind. Dieses Kapitel beschreibt auch das Konfigurieren von Werten für Variablen, die für anwenderspezifische Operatorgruppen definiert werden können.

Hinweis: Sie müssen keine Module (Operatorkategorien) konfigurieren. Die empfohlene Best Practice besteht darin, dass der Inhaltsdesigner globale Datensätze für die Moduleinstellungen erstellt. Danach verwendet der Inhaltsdesigner Ausdrücke, die sich auf die Datensatzvariablen in den Operatoreigenschaften beziehen.

Dieses Kapitel enthält folgende Themen:

Operatorkategorien und Operatorordner

Operatorkategorien entsprechen den Operatorordnern. Administratoren konfigurieren Operatorkategorien auf der Registerkarte "Module" und beginnen auf der Domänenebene. Inhaltsdesigner erweitern die Operatorordner, um eine Gruppe der Operatoren in der genannten Kategorie anzuzeigen. Operatorordner werden im Auswahlmenü "Operatoren" auf der Registerkarte "Designer" angezeigt.

Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf die Registerkarte "Module", um die Operatorkategorien unter "Name" aufzulisten.

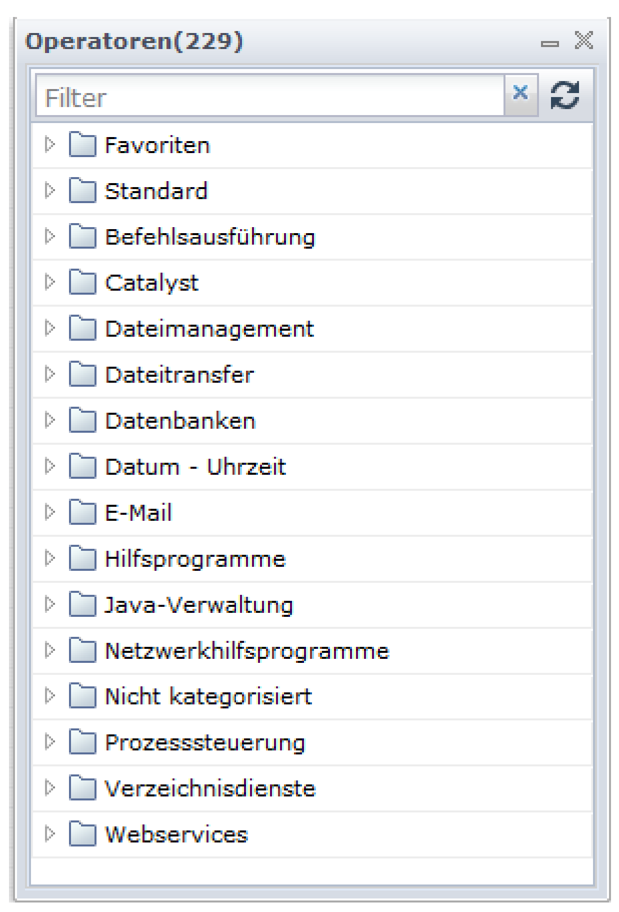
Hinweis: Die Liste "Name" enthält auch veröffentlichte Gruppen, die für anwenderspezifische Operatoren erstellt werden. Inhaltsdesigner können diese Gruppenordner erweitern, um eine Gruppe der anwenderspezifischen Operatoren in der genannten Konfigurationsgruppe anzuzeigen. Konfigurations-Gruppenordner, die hier für anwenderspezifische Operatoren angezeigt werden, werden auch im Auswahlmenü "Operatoren" auf der Registerkarte "Designer" angezeigt.

Inhalt von "Domäne"

Sicherheit | Eigenschaften | Module | Auslöser | Audit-Pfade

Name	Beschreibung
Befehlsausführung	Führt Programme und Skripten in Umgebungen des Host-Betriebssystems aus.
Catalyst	Bietet Zugriff auf Catalyst-Connectors
Dateimanagement	Dieses Modul überwacht Dateien und Verzeichnisse und deren Inhalte.
Dateitransfer	Ermöglicht Dateitransfer (FTP/SFTP).
Datenbanken	Dies ist das Datenbankmodul für die Kommunikation mit mehreren Datenbankservern.
Datum - Uhrzeit	Führt Zeit- und Kalendereinschränkungen in CA Process Automation-Prozessen aus.
E-Mail	Dies ist der Maildienst, der E-Mails über IMAP- oder POP3-Protokolle vom Server abruft.
Hilfsprogramme	Dieses Modul besteht aus Dienstprogrammoperatoren, die in PAM-Prozessen verwendet werden.
Java-Verwaltung	Bietet eine Verwaltungsschnittstelle mit externen Systemen, die JMX unterstützen.
Netzwerkhilfsprogramme	Bietet Hilfsprogramme und Betriebsabläufe für Netzwerkdienste.
Prozesssteuerung	Führt CA Process Automation-Prozess aus, überwacht sie und steuert sie.
Verzeichnisdienste	Bietet eine Schnittstelle zur Unterstützung von LDAP/AD.
Webservices	Bietet eine Schnittstelle zu externen, durch SOAP zur Verfügung gestellten Services.

Klicken Sie auf die Registerkarte "Designer" und auf "Anzeigen", und wählen Sie Operatoren aus. Die angezeigten Ordnernamen stellen die gleiche Operatorgruppierung wie die Operatorkategorien dar, die Sie konfigurieren.



Inhaltsdesigner wählen Operatoren aus dem Auswahlmenü "Operatoren" aus, um automatisierte Prozesse zu erstellen. Jeder Operator führt eine bestimmte Operation aus. Damit Designer den erforderlichen Operator schneller finden kann, werden Operatoren durch CA Process Automation nach häufig verwendeten Kategorien gruppiert. Zum Beispiel werden alle Operatoren, die für eine Dateiübertragung mit FTP verwendet werden, in einen Ordner mit dem Namen "Dateiübertragung" gruppiert.

Sie konfigurieren die Werte der Operatorkategorie auf Domänenebene. Die Werte werden auf Umgebungsebene und anschließend auf der Ebene des Koordinationsrechners oder auf der Ebene des Agentenkontaktpunkts geerbt. Sie können geerbte Werte auf jeder Ebene überschreiben. Die Operatoren erben dann die Standardwerte der Operatorkategorien. Inhaltsdesigner können diese Werte akzeptieren oder überschreiben.

Weitere Informationen:

Kategorienkonfiguration und Operatorvererbung (siehe Seite 326)

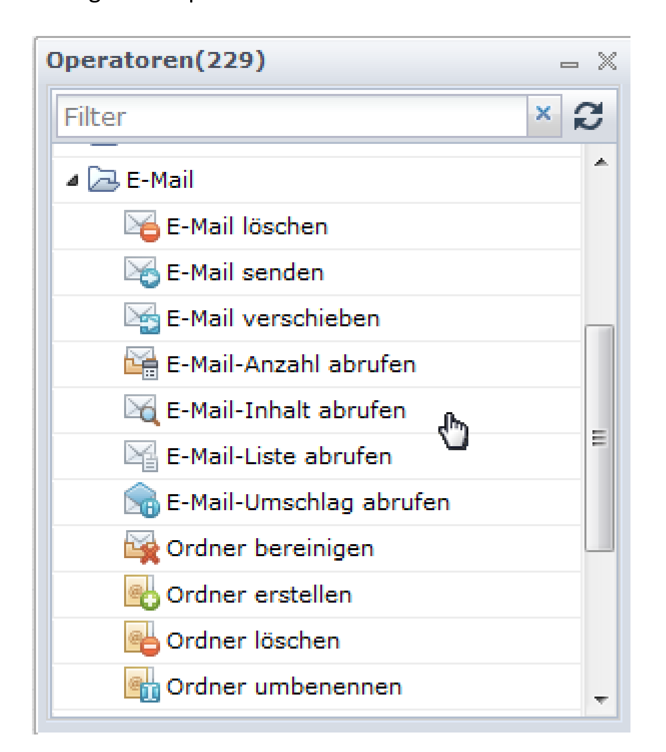
Beispiel: Kategorieneinstellungen, die vom Operator verwendet werden

Wenn Sie Domänenebeneneinstellungen für jede Kategorie auf der Registerkarte "Module" konfigurieren, berücksichtigen Sie die Werte, die normalerweise von Operatoren verwendet werden. Wenn Sie Einstellungen konfigurieren, die auf dem häufigsten Anwendungsfall basiert, so wird die Konfiguration auf niedrigen Ebenen nur für Ausnahmen durchgeführt.

Berücksichtigen Sie die Konfiguration in den E-Mail-Eigenschaften, in denen "Standardmäßiges Verbindungsprotokoll" auf "IMAP" und "Standardmäßiger Mailserverport" auf "143" festgelegt ist. Sie konfigurieren den standardmäßigen Mailserver, den standardmäßigen Anwendernamen und das standardmäßige Kennwort.



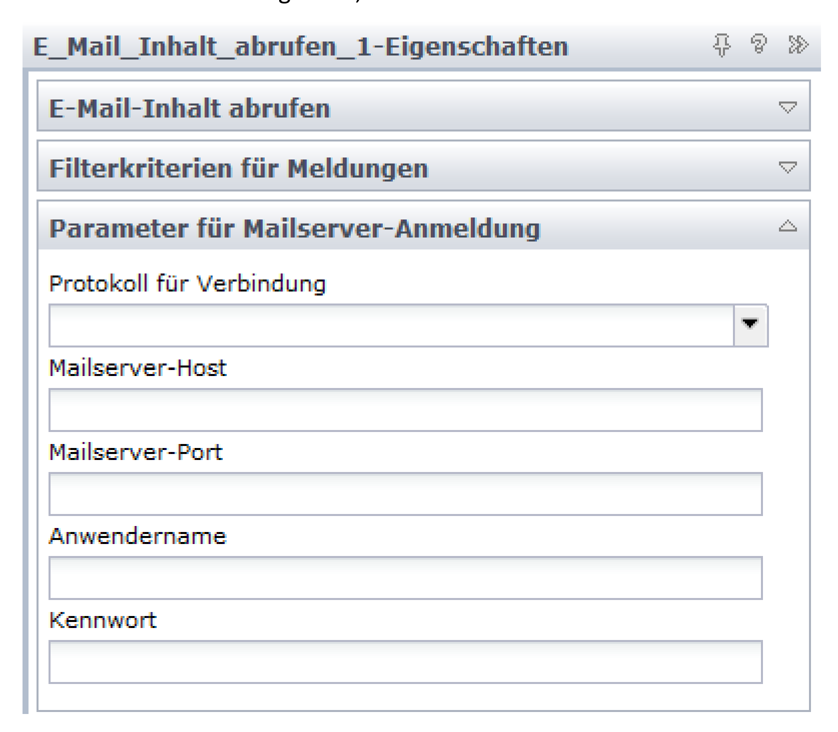
Wenn ein Inhaltsdesigner einen Prozess für E-Mails automatisiert, ist einer der verfügbaren Operatoren "E-Mail-Inhalt abrufen".



Wenn ein Inhaltsdesigner den Operator "E-Mail-Inhalt abrufen" auf die Arbeitsfläche zieht, werden die Eigenschaften "Get_Email_Content_1" angezeigt. Beachten Sie die Ähnlichkeit zwischen den E-Mail-Eigenschaften auf der Registerkarte "Module" der Registerkarte "Konfiguration" und den Anmeldeparametern für den Mail-Server für die Eigenschaften "Get_Email_Content_1", die auf der Registerkarte "Designer" angezeigt werden.

Der Operator "E-Mail-Inhalt abrufen" übernimmt Werte für diese Anmeldeparameter für den Mail-Server	von Werten, die in der E-Mail-Moduleinstellung für E-Mail-Eigenschaften konfiguriert wurden
Protokoll für Verbindung	Standardmäßiges Protokoll für Verbindung
Mailserver-Host	Standardmäßiger Mailserverhost
Mailserver-Port	Standardmäßiger Mailserverport
Anwendername	Standardmäßiger Anwendername
Kennwort	Standardmäßiges Kennwort

Der Inhaltsdesigner kann prozessspezifische Werte konfigurieren und zuvor konfigurierte Standardwerte überschreiben. Oder der Inhaltsdesigner kann das Feld leer lassen, um die Standardwerte zu übernehmen. In diesem Beispiel verwendet ein leeres Protokoll für Verbindung IMAP, und ein leerer Mailserver-Port verwendet Port 143.



Konfigurieren der Operatorkategorien

Administratoren, die die Domäne sperren können, können Standardeinstellungen für Operatorkategorien auf Domänenebene konfigurieren oder ändern. Diese Konfigurationen werden vererbt. Sie können diese Einstellungen auf den Umgebungs-, Koordinationsrechner- und Agentebenen bearbeiten. Weitere Informationen finden Sie unter Überschreiben übernommener Einstellungen einer Kategorie von Operatoren (siehe Seite 330).

Werte für alle Felder für Operatorkategorien können auf Operatorebene überschrieben werden. Die Werte, die Sie für Operatorkategorien eingeben, sind immer Standardwerte. Wenn ein SSH-Operator mit einem leeren Feld konfiguriert ist, vererbt dieser Operator den Standardwert des entsprechenden Felds aus der Kategorieeinstellung. Wenn Sie eine Auswahl eines Werts auf der Registerkarte "Modul" vornehmen, wird nichts aktiviert oder deaktiviert. Sie können alle Standards nach eigenem Ermessen angeben. (Wenn Sie diese gleichen Optionen auf der Operatorebene konfigurieren, deaktiviert die Auswahl einer Option die Auswahl einer anderen Option.)

Hinweis: Weitere Informationen zur Operatorkonfiguration dieser Felder finden Sie im *Referenzhandbuch für Inhaltsdesign*.

Um ein Feld für eine Eingabe, die länger ist als der angegebene Speicherplatz, zu erweitern, klicken Sie mit der rechten Maustaste auf das Feld, und wählen Sie "Erweitern" aus. Ein Dialogfeld mit einem Textfeld wird geöffnet.

Informationen zu Catalyst

Catalyst ist mit den folgenden Einstellungen konfiguriert:

- Catalyst-Eigenschaftseinstellungen.
- Catalyst-Sicherheitseinstellungen.

Das vereinheitlichte Servicemodell (USM) ist ein Schema von allgemeinen Objekttypen und Eigenschaften, in die Daten von allen Connectors konvertiert werden. Das USM-Schema ermöglicht die Analyse von Daten von allen Domänen-Managern aus. Sie können Daten in einer allgemeinen Schnittstelle mit identischer Formatierung über die Domänen-Manager hinweg analysieren.

Die Catalyst-Operatoren ermöglichen es Ihnen, in automatisierten Prozessen Catalyst-Connectors zu verwenden. Die Catalyst-Operatoren unterstützen die folgenden Schnittstellen:

- Create, read, update, delete (CRUD)
- Ausführen
- Event-Abonnement

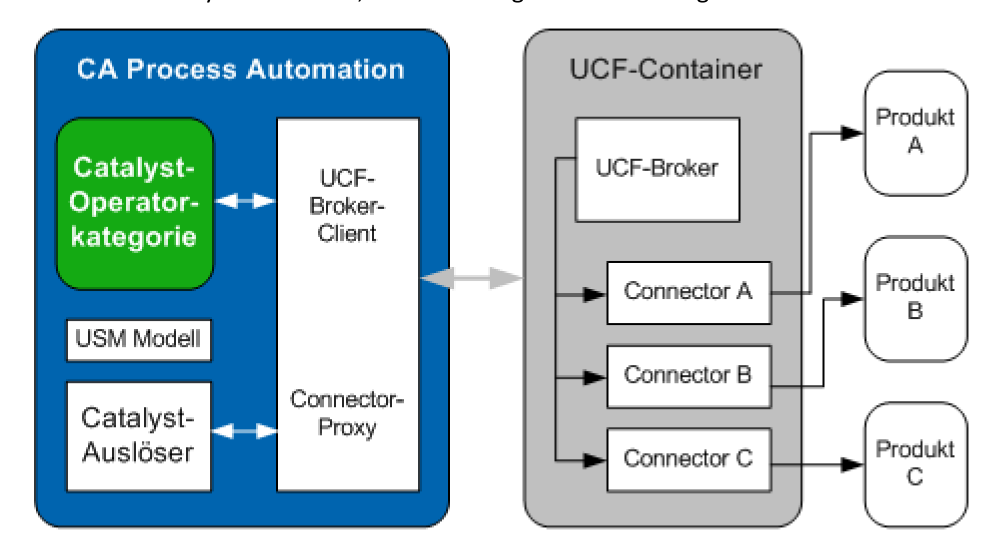
Die Operatoren zeigen USM-Objekttypen und -Eigenschaften des an.

Wenn ein allgemeines USM-Modell und standardmäßige UCF-Schnittstellen verwendet werden, ist Catalyst mit allen UCF-Connectors und -Containern kompatibel.

CA Process Automation bettet die folgenden UCF-USM-Komponenten ein:

- Catalyst Operator-Kategorie
- Catalyst-Auslöser

Die Operatorkategorie "Catalyst" und der Catalyst-Auslöser sind Remote-UCF-Connector-Clients. Sie verwenden den UCF-Broker- und die Connector-Proxy-Schnittstelle, wie in der folgenden Abbildung veranschaulicht:



Konfigurieren von Catalyst-Standards

Sie können Catalyst-Standards durch das Ausfüllen der folgenden Registerkarten konfigurieren:

- Standardmäßige Catalyst-Eigenschaften
- Standardmäßige Catalyst-Sicherheit
- Standardmäßige Catalyst-Ansprüche
- Standardmäßige Catalyst-Kennwortansprüche

Hinweis: Die Kennwortwerte sind verschlüsselt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Catalyst, und wählen Sie Bearbeiten aus.

   Die Registerkarte Standardmäßige Catalyst-Eigenschaften wird geöffnet.
3. Konfigurieren Sie die standardmäßigen Catalyst-Eigenschaften.
   a. Geben Sie die entsprechende Standard-URL im Feld UCF-Broker-URL ein. Der zugeordnete Operator erbt diese Einstellung. Beispiele für URLs für normale und sichere Verbindungen:

      `http://`*`hostname`*`:7000/ucf/BrokerService`

      `https://`*`hostname`*`:7443/ucf/BrokerService`
   b. Geben Sie den entsprechenden Namen im Feld "Name der Produkteigenschaften-Konfigurationsdatei" ein. Diese Datei wird verwendet, um Eigenschaften anzupassen, die im generischen Operator "Erstellen" angezeigt werden.
4. Klicken Sie auf die Registerkarte Standardmäßige Catalyst-Sicherheit, und geben Sie die standardmäßigen Werte für ID und Kennwort des Catalyst-Anwenders ein.
5. Klicken Sie auf die Registerkarte Standardmäßige Catalyst-Ansprüche, und schließen Sie die Konfiguration ab.
   a. Klicken Sie auf Parameter hinzufügen, und geben Sie den Namen des ersten Anspruchs und dessen Wert ein.
   b. Wiederholen Sie diesen Schritt für jeden standardmäßigen Anspruch.
   c. Verwenden Sie die Auf- und Abwärtspfeile, um die Ansprüche nach Bedarf sequenziell zu ordnen.

6. Klicken Sie auf die Registerkarte Standardmäßige Catalyst-Kennwortansprüche, und schließen Sie die Konfiguration ab.
   a. Klicken Sie auf Parameter hinzufügen, und geben Sie den Namen des ersten Anspruchs und dessen Wert ein.
   b. Wiederholen Sie diesen Schritt für jeden standardmäßigen Kennwortanspruch.
   c. Verwenden Sie die Auf- und Abwärtspfeile, um die Ansprüche nach Bedarf sequenziell zu ordnen.
7. Klicken Sie auf Speichern und Schließen.
8. Klicken Sie auf "Speichern".
9. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Laden von Catalyst-Deskriptoren

Ein Catalyst-Connector-Deskriptor gibt die Funktionen des Connectors, einschließlich der Vorgänge, die unterstützt werden, an. Jeder Betriebsablauf gibt außerdem die zugeordneten Parameter an. Sie können Deskriptoren in CA Process Automation laden. Der Operator "Ausführen", ein Operator in der Operatorkategorie "Catalyst", verwendet die Deskriptoren. Das Produkt zeigt die geladenen Deskriptoren auf verschiedenen Ebenen an:

- Betriebsablaufkategorie (Drop-down)
- Betriebsablauf (Drop-down)
- Parameter (Editorwerte)

Sie können einen Catalyst-Deskriptor von Ihrem lokalen Host in den Remote-Domänen-Koordinationsrechner als Anwenderressource laden. Das Produkt reproduziert alle Ressourcen zu jedem neuen Koordinationsrechner.

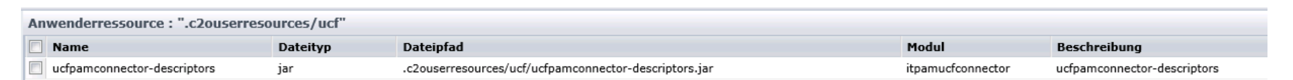
Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie "Anwenderressourcen verwalten" im linken Bereich.
3. Erweitern Sie den Ordner "Repository", blenden Sie den Ordner "Anwenderressource" ein, und wählen Sie dann den Ordner "ucf" aus. If
4. Klicken Sie auf Neu.
5. Füllen Sie die Felder im Bereich "Neue Ressource hinzufügen" nach Bedarf aus.

   Hinweis: Lassen Sie das Feld "Pfad zu Ressourcen-Unterordner" leer. Schritt 3, der im Pfad des Unterordners "ucf" angegeben ist.

6. Klicken Sie auf "Speichern".

   Die Liste der Anwenderressourcen zeigt den Deskriptor an.



Anwenderressource : ".c2ouserresources/ucf"

Name	Dateityp	Dateipfad	Modul	Beschreibung
ucfpamconnector-descriptors	jar	.c2ouserresources/ucf/ucfpamconnector-descriptors.jar	itpamucfconnector	ucfpamconnector-descriptors

Hinweis: Der Deskriptor ist im Operator "Ausführen" verfügbar, nachdem Sie den Koordinationsrechner neu starten. Weitere Informationen über den Operator "Ausführen" in der Kategorie "Catalyst" finden Sie im *Referenzhandbuch für Inhaltsdesign*.

Weitere Informationen:

Hinzufügen einer Ressource zu Anwenderressourcen (siehe Seite 356)

Info zur Befehlsausführung

Befehlsausführungs-Operatoren ermöglichen Ihnen das Ausführen von Shell-Skripts oder ausführbaren Programmen auf allen Agenten oder Koordinationsrechnern. Diese Kategorie stellt Daten- und Ressourcenzugriff für Netzwerkgeräte bereit, die das Telnet und SSH-Schnittstellenprotokolle (Secure Shell) unterstützen.

Es folgt eine Liste der Operatoren:

- Programm ausführen
- Skript ausführen
- SSH-Befehl ausführen
- SSH-Skript ausführen
- Telnet-Befehl ausführen
- Telnet-Skript ausführen

Wenn Sie Skripts ausführen, folgen Sie den Windows- oder UNIX-Betriebssystemkonventionen, um sie ausführbar zu machen. In CA Process Automation geben Skripts Ergebnisse als CA Process Automation-Datensatzvariablen zurück.

- Für UNIX-Systeme gibt die Anfangszeile des Skript den vollständigen Pfad zum gewünschten Interpreter an. Beispiel:

  `#!/bin/sh`

  Gibt die Ausführung mithilfe von sh an, die Bourne-Shell auf Systemen wie Oracle Solaris. Auf Linux-Systemen ist diese Eingabe eine Verknüpfung zu einer anderen Shell, zum Beispiel zur Bash-Shell. Ein Skript-Operator kann alle Skripts ausführen, für die der Zielhost über einen Interpreter verfügt.

  Shell-Befehle, beispielsweise *cp* oder *dir,* müssen in eine ausführbare Skriptdatei eingebettet werden.

  `#!/usr/bin/perl`

  Bei Platzierung an den Anfang eines Perl-Skripts erfährt der Webserver, wo sich die ausführbare Perl-Datei befindet.

- Für Windows-Systeme definiert die Dateinamenerweiterung den Skripterstellungsinterpreter. Definieren Sie für Windows Dateizuordnungen, um die Skripts automatisch auszuführen. Die folgenden Erweiterungen werden unterstützt:

  `*.ps1`

  Eine Windows-PowerShell-Datei.

  `*.exe`

  Eine ausführbare Datei, die Programme und Routinen installiert und ausführt.

  `*.cmd`

  Eine aus einer Sequenz von Befehlen bestehende Stapeldatei. Ähnelt einer .BAT-Datei, wird aber vom Programm "CMD.exe" anstatt von "COMMAND.com" ausgeführt.

  `*.vbs`

  VBScript-Datei.

  `*.wsh`

  Eine Windows Script Host-Textdatei mit Parametern für ein Skript, wie z. B. eine .vbs-Datei; benötigt Microsoft WScript oder Microsoft CScript, um die Datei zu öffnen.

Konfigurieren der Befehlsausführung: Standardmäßige SSH-Eigenschaften

Wenn Sie standardmäßige SSH-Eigenschaften konfigurieren, konfigurieren Sie folgende Elemente:

- Die Spezifikationen des Terminaltyps
- Die Authentifizierungsdetails für das Anmelden bei einem Remote-Host
- (Optional) Ob Anwender nach der Anmeldung gewechselt werden sollen

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Befehlsausführung, und wählen Sie Bearbeiten aus.
3. Wählen Sie die Registerkarte "Standardmäßige SSH-Eigenschaften" aus.
4. Wählen Sie den Pseudoterminaltyp aus, der bei SSH-Verbindungen abgefragt wird.

   Hinweis: VT100 arbeitet normalerweise mit Linux-Hosts, während VT400 normalerweise mit Windows-Hosts arbeitet.
5. Wählen Sie den Standardport aus, der für die Verbindung mit dem Remote-Host verwendet werden soll.

   Hinweis: Port 22 ist der systemeigene TCP-/UDP-Port für das Secure Shell-Protokoll (SSH).
6. Geben Sie den Standardwert für den Anwendernamen an, der für die Anmeldung beim Remote-Host verwendet werden soll.
7. Geben Sie die privaten Schlüsselstandards an:
   a. Geben Sie an, ob ein privater Schlüssel für die Anmeldung verwendet werden soll.

      Hinweis: Die Alternative besteht darin, die Kennwortinformationen zu verwenden.

   b. Geben Sie das Standardkennwort an, der für die Anmeldung beim Remote-Host verwendet werden soll.

   c. Klicken Sie auf "Durchsuchen" (...), und rufen Sie den Inhalt des privaten Schlüssels ab, das heißt, den Inhalt eines standardmäßigen privaten Schlüssels für die Anmeldung beim Remote-Host.

   d. Geben Sie den Pfad zu einem standardmäßigen privaten Schlüssel für die Anmeldung beim Remote-Host ein.

e. Geben Sie die Passphrase ein, die verwendet wird, um den Inhalt des privaten Schlüssels zu entsperren.

   Hinweis: Diese Passphrase ist erforderlich, wenn der private Schlüssel mit einer Passphrase erstellt wurde.

8. Geben Sie die Standards für die Ausführung des Skripts oder angegebener Befehle als ein anderer Anwender an.

   a. Geben Sie an, ob das Skript oder die angegebenen Befehle als anderer Anwender ausgeführt werden sollen.

   b. Geben Sie den betriebssystemspezifischen Befehl für den Anwenderwechsel auf dem Remote-Host an. Der Befehl "su -root" wechselt Anwender zum Root-Anwender. Zum Beispiel:

      ```
      su - <Anwendername>
      ```

      ```
      sudo su - <Anwendername>
      ```

   c. Geben Sie einen regulären Ausdruck für die standardmäßige Textaufforderung ein, wenn der Remote-Host ein Kennwort für das Wechseln von Anwendern benötigt.

      Die Textaufforderung ist normalerweise "Kennwort:" oder "kennwort:". Der reguläre Ausdruck, ".*ennwort:" findet alle Eingaben (einschließlich neuer Zeilen) und ein großgeschriebenes "K" oder ein kleingeschriebenes "k", gefolgt von "ennwort:".

   d. Geben Sie das Standardkennwort für die standardmäßige Textaufforderung ein, wenn der Remote-Host ein Kennwort für das Wechseln von Anwendern benötigt.

   e. Geben Sie einen regulären Ausdruck für die Befehlsaufforderung an, die angibt, dass der Remote-Host nach einem Anwenderwechsel für Befehle bereit ist.

      Übliche Eingabeaufforderungen sind # (Hash), > (Größer als) und ? (Fragezeichen). Die Eingabe ".*[$>?:#]" stimmt mit sämtlichen Eingaben (einschließlich neuer Zeilen) überein, auf die #, >, ?, $ (Dollarzeichen) oder : (Doppelpunkt) folgen. Lesen Sie sich folgende Beispiele sorgfältig durch:

      ```
      .*[$]
      ```

      ```
      .*[$>?:#]
      ```

      Hinweis: Wenn Sie ein Dollarzeichen in einem regulären Ausdruck verwenden, schließen Sie es in eckige Klammern ein. Ein Dollarzeichen ohne Klammern hat eine Sonderbedeutung bei regulären Ausdrücken.

9. Klicken Sie auf Speichern und Schließen.

10. Klicken Sie auf "Speichern".

11. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren der Befehlsausführung: Standardmäßige Telnet-Eigenschaften

Die Konfiguration der standardmäßigen Telnet-Eigenschaften umfasst die folgenden Aufgaben:

- Konfigurieren der Konnektivität
- Angeben des Anmeldeschemas und damit verbundener Details
- Angeben, ob Anwender nach Anmeldung beim Remote-Host gewechselt werden sollen
- Definieren der Details für Anwenderwechsel

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Befehlsausführung, und wählen Sie Bearbeiten aus.
3. Wählen Sie auf der Registerkarte Standardmäßige Telnet-Eigenschaften das standardmäßige Pseudoterminal aus, das bei der Telnet-Verbindung abgefragt werden soll.
4. Wählen Sie den Standardport aus, der für die Verbindung mit dem Remote-Host verwendet werden soll.

   Hinweis: Port 23 ist der bekannte TCP-/UDP-Port für Telnet.
5. Verwenden Sie für Zeitlimit für Verbindung (Sek.) das Spinner-Feld, um das Intervall (in Sekunden) auszuwählen, während dessen gewartet wird, bis die Verbindung anläuft.
6. Wählen Sie ein standardmäßiges Anmeldeschema aus der Drop-down-Liste aus.
7. Definieren Sie die standardmäßigen Werte und Aufforderungen für die Anmeldung:
   a. Geben Sie einen regulären Ausdruck für die Anmeldeaufforderung an (geben Sie zum Beispiel ".*ogin.*:" ein).
   b. Geben Sie den Anwendernamen an, der für die Anmeldung beim Remote-Host verwendet werden soll.
   c. Geben Sie einen regulären Ausdruck für die standardmäßige Textaufforderung an, der anzeigt, dass der Remote-Host ein Kennwort für das Anmelden des Anwenders benötigt (geben Sie zum Beispiel ".*assword.*:" ein).
   d. Geben Sie das standardmäßige Kennwort an, das für die Anmeldung beim Remote-Host verwendet wird.

8. Geben Sie einen regulären Ausdruck für die Eingabeaufforderung an, die angibt, dass der Remote-Host für Befehle vorbereitet ist (geben Sie zum Beispiel ".*[$>?:#]" ein).

   Hinweis: Um ein Dollarzeichen in einem regulären Ausdruck zu verwenden, schließen Sie es in eckige Klammern ein. Beispiel: [$].

9. Wählen Sie das Intervall (in Sekunden) aus, während dessen die Verbindung auf die Aufforderung zum Senden der Befehle wartet.

10. Definieren Sie die Standardwerte für Anwenderwechsel:

    a. Geben Sie an, ob ein Anwenderwechsel durchgeführt werden soll, bevor das Skript oder die angegebenen Befehle ausgeführt werden.

    b. Geben Sie den betriebssystemspezifischen Befehl ein, mit dem Anwender auf dem Remote-Host gewechselt werden sollen.

       Hinweis: Der Befehl "su -root" ändert den Anwender in den Root-Anwender um.

       Lesen Sie sich folgende Beispiele sorgfältig durch:

       ```
       su - <Anwendername>
       ```

       ```
       sudo su - <Anwendername>
       ```

    c. Geben Sie einen regulären Ausdruck für die standardmäßige Textaufforderung für das Kennwort für Anwenderwechsel an (geben Sie zum Beispiel ".*assword.*:" ein).

    d. Geben Sie das Standardkennwort ein, das in der Textaufforderung für das Kennwort eingegeben werden soll.

    e. Geben Sie einen regulären Ausdruck für die Eingabeaufforderung an, die angibt, dass der Remote-Host nach einem Anwenderwechsel für Befehle bereit ist.

       Hinweis: Hash (#), Größer als (>) und Fragezeichen (?) sind die üblichen Eingabeaufforderungen. Geben Sie ".*[$>?:#]" ein, um mit sämtlichen Eingaben (einschließlich neuer Zeilen) übereinzustimmen, auf die #, >, ?, $ (Dollarzeichen) oder : (Doppelpunkt) folgen.

       Lesen Sie sich folgende Beispiele sorgfältig durch:

       ```
       .*[$]
       ```

       ```
       .*[$>?:#]
       ```

       Hinweis: Um ein Dollarzeichen in einem regulären Ausdruck zu verwenden, schließen Sie es in eckige Klammern ein. Beispiel: [$].

11. Klicken Sie auf Speichern und Schließen.

12. Klicken Sie auf "Speichern".

13. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren der Befehlsausführung: Standardmäßige Eigenschaften der UNIX-Befehlsausführung

Sie können standardmäßige Ausführungseigenschaften für die UNIX-Befehle konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Befehlsausführung, und wählen Sie Bearbeiten aus.
3. Wählen Sie die Registerkarte Standardmäßige Eigenschaften der UNIX-Befehlsausführung aus.
4. Geben Sie einen der folgenden Kommandozeileninterpreter als Standard für das Profil und für Shell-Befehle an:

   `/bin/bash`

   `/bin/csh`

   `/bin/ksh`
5. Geben Sie den Namen der standardmäßigen Shell-Skriptdatei ein, die interpretiert werden soll, bevor ein Anwenderprozess startet, für den kein Profil angegeben ist.

   Das Profil kann alle nicht interaktiven Befehle enthalten, die der Shell-Interpreter versteht.

6. Geben Sie die Standardwerte für Anwenderanmeldeinformationen an.

   a. Wählen Sie einen der folgenden Werte aus, um anzugeben, dass die Prozessoperatoren die ausgewählte Option verwenden, wenn keine Anmeldeinformationen angegeben sind:

      ■ (Standard) Ist standardmäßig der Anwender, unter dem der Kontaktpunkt ausgeführt wird.

        Die Prozessoperatoren verwenden die Anmeldeinformationen, unter denen der Agenten- oder Koordinationsrechnerprozess ausgeführt wird.

      ■ Ist standardmäßig der angegebene Standardanwender.

        Die Prozessoperatoren verwenden die Anmeldeinformationen, die als Standardanwender und Standardkennwort konfiguriert sind.

      ■ Kein Standard.

        Die Prozessoperatoren verwenden die zur Laufzeit bereitgestellten Anmeldeinformationen.

   b. Berücksichtigen Sie die Implikationen der Angabe von Standards für Anwender-ID und Kennwort:

      ■ Damit Anwender keine Prozesse über CA Process Automation definieren und starten können, auf die sie sonst keinen Zugriff haben, geben Sie eine Anwender-ID ein, die nur über notwendige Berechtigungen verfügt.

      ■ Lassen Sie die Anwender-ID und das Kennwort leer, um Anwender zu zwingen, diese Werte anzugeben, wenn sie Prozesse über CA Process Automation starten.

   c. Geben Sie bei Bedarf das Shell-Konto an, das verwendet werden soll, wenn Prozesse ohne Anwendernamen und Kennwort gestartet werden.

   d. Geben Sie bei Bedarf das Kennwort für das Shell-Anwenderkonto ein.

      Hinweis: Kennwörter, die Teil von Befehlsausführungs-Konfigurationen sind, werden geschützt und können durch kein Programm geändert werden, das an externe Methoden weitergegeben oder auf das durch externe Methoden verwiesen wird.

   e. Geben Sie das standardmäßige Kennwort zur Bestätigung noch einmal ein.

7. Berücksichtigen Sie die Implikationen der Angabe von Standards für Anwender-ID und Kennwort:

   ■ Damit Anwender keine Prozesse über CA Process Automation definieren und starten können, auf die sie sonst keinen Zugriff haben, geben Sie eine Anwender-ID ein, die nur über notwendige Berechtigungen verfügt.

   ■ Lassen Sie die Anwender-ID und das Kennwort leer, um Anwender zu zwingen, diese Werte anzugeben, wenn sie Prozesse über CA Process Automation starten.

8. Geben Sie bei Bedarf das Shell-Konto an, das verwendet werden soll, wenn Prozesse ohne Anwendernamen und Kennwort gestartet werden.

9. Geben Sie bei Bedarf das Kennwort für das Shell-Anwenderkonto ein.

   Hinweis: Kennwörter, die Teil von Befehlsausführungs-Konfigurationen sind, werden geschützt und können durch kein Programm geändert werden, das an externe Methoden weitergegeben oder auf das durch externe Methoden verwiesen wird.

10. Geben Sie das standardmäßige Kennwort zur Bestätigung noch einmal ein.

11. Geben Sie an, ob das Anwenderprofil, das dem angegebenen Standardanwender und Standardkennwort zugeordnet ist, geladen werden soll.

12. Geben Sie an, ob Sie die Kennwortüberprüfung deaktivieren möchten.

13. Klicken Sie auf Speichern und Schließen.

14. Klicken Sie auf "Speichern".

15. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren der Befehlsausführung: Standardmäßige Eigenschaften der Windows-Befehlsausführung

Sie können standardmäßige Ausführungseigenschaften für die Windows-Befehle konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".

2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Befehlsausführung, und wählen Sie Bearbeiten aus.

3. Wählen Sie die Registerkarte "Standardmäßige Eigenschaften der Windows-Befehlsausführung" aus.

4. Geben Sie die standardmäßigen Kommandozeileninterpreter für die Verwendung für das Profil und für Shell-Befehle an. Zum Beispiel:

   ```
   cmd.exe
   ```

   Hinweis: Geben Sie nicht "Command.exe" ein.

5. Geben Sie den Namen der standardmäßigen Shell-Skriptdatei ein, die interpretiert werden soll, bevor ein Anwenderprozess startet, für den kein Profil angegeben ist.

   Der Kommandozeileninterpreter, den das Shell-Programm angibt, interpretiert die Profildatei. Das Profil kann alle nicht interaktiven Befehle enthalten, die der Shell-Interpreter versteht.

6. Geben Sie die Standardwerte für Anwenderanmeldeinformationen an.
   a. Wählen Sie einen der folgenden Werte aus, um anzugeben, dass die Prozessoperatoren die ausgewählte Option verwenden, wenn keine Anmeldeinformationen angegeben sind:
      - (Standard) Ist standardmäßig der Anwender, unter dem der Kontaktpunkt ausgeführt wird.

        Die Prozessoperatoren verwenden die Anmeldeinformationen, unter denen der Agenten- oder Koordinationsrechnerprozess ausgeführt wird.
      - Ist standardmäßig der angegebene Standardanwender.

        Die Prozessoperatoren verwenden die Anmeldeinformationen, die als Standardanwender und Standardkennwort konfiguriert sind.
      - Kein Standard.

        Die Prozessoperatoren verwenden die zur Laufzeit bereitgestellten Anmeldeinformationen.
   b. Berücksichtigen Sie die Implikationen der Angabe von Standards für Anwender-ID und Kennwort:
      - Damit Anwender keine Prozesse über CA Process Automation definieren und starten können, auf die sie sonst keinen Zugriff haben, geben Sie eine Anwender-ID ein, die nur über notwendige Berechtigungen verfügt.
      - Lassen Sie die Anwender-ID und das Kennwort leer, um Anwender zu zwingen, diese Werte anzugeben, wenn sie Prozesse über CA Process Automation starten.
   c. Geben Sie bei Bedarf das Shell-Konto an, das verwendet werden soll, wenn Prozesse ohne Anwendernamen und Kennwort gestartet werden.
   d. Geben Sie bei Bedarf das Kennwort für das Shell-Anwenderkonto ein.

      Hinweis: Kennwörter, die Teil von Befehlsausführungs-Konfigurationen sind, werden geschützt und können durch kein Programm geändert werden, das an externe Methoden weitergegeben oder auf das durch externe Methoden verwiesen wird.
   e. Geben Sie das standardmäßige Kennwort zur Bestätigung noch einmal ein.
7. Berücksichtigen Sie die Implikationen der Angabe von Standards für Anwender-ID und Kennwort:
   - Damit Anwender keine Prozesse über CA Process Automation definieren und starten können, auf die sie sonst keinen Zugriff haben, geben Sie eine Anwender-ID ein, die nur über notwendige Berechtigungen verfügt.
   - Lassen Sie die Anwender-ID und das Kennwort leer, um Anwender zu zwingen, diese Werte anzugeben, wenn sie Prozesse über CA Process Automation starten.

8. Geben Sie bei Bedarf das Shell-Konto an, das verwendet werden soll, wenn Prozesse ohne Anwendernamen und Kennwort gestartet werden.
9. Geben Sie bei Bedarf das Kennwort für das Shell-Anwenderkonto ein.

   Hinweis: Kennwörter, die Teil von Befehlsausführungs-Konfigurationen sind, werden geschützt und können durch kein Programm geändert werden, das an externe Methoden weitergegeben oder auf das durch externe Methoden verwiesen wird.
10. Geben Sie das standardmäßige Kennwort zur Bestätigung noch einmal ein.
11. Geben Sie an, ob das Anwenderprofil, das dem angegebenen Standardanwender und Standardkennwort zugeordnet ist, geladen werden soll.
12. Klicken Sie auf Speichern und Schließen.
13. Klicken Sie auf "Speichern".
14. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Informationen zu Datenbanken

Die Operatoren-Kategorie "Datenbanken" verwendet die Java Database Connectivity (JDBC)-Technologie. JDBC-Technologie unterstützt Konnektivität in einer heterogenen Umgebung zwischen der Programmiersprache "Java" und Datenbanken wie z. B. Microsoft SQL Server. Die Kategorie "Datenbanken" unterstützt keine Verwaltungsoperationen, wie das Anhalten eines Datenbankservers. Die Verbindungsinformationen können mit dem Server, Port und der System-ID (SID) oder mit einem TNSNAMENS-Eintrag in "tnsnames.ora" angegeben werden. Die Datei "tnsnames.ora" ist die Namenskonfigurationsdatei von Oracle Service.

Die Kategorie "Datenbanken" schließt Einstellungen für die folgenden Datenbanken ein:

- Oracle
- MSSQL
- MySQL
- Sybase

Installieren Sie den entsprechenden Treiber, um die Operatoren-Kategorie "Datenbanken" mit einem RDBMS eines anderen Anbieters zu verwenden, der nicht von CA Process Automation verwendet wird.

Hinweis: Weitere Informationen finden Sie im *Installations- und Konfigurationshandbuch* unter "JDBC-Treiber für JDBC-Connectors".

Weitere Informationen:

Aktivieren von "Integrierte Sicherheit von Windows" für das JDBC-Modul für MSSQL Server (siehe Seite 307)

Konfigurieren von Datenbanken: Standardmäßige Oracle-Eigenschaften

Sie können die Operatoren-Kategorie "Datenbanken" für Oracle konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Datenbanken, und wählen Sie Bearbeiten aus.
3. Wählen Sie auf der Registerkarte Standardmäßige Oracle-Eigenschaften einen der folgenden Werte als standardmäßigen Oracle JBDC-Treibertyp aus. Verwenden Sie eine JDBC-Version, die mit Ihrer Version des Java Development Kit (JDK) übereinstimmt.

   thin

   Der Thin-Treibertyp wird auf der Client-Seite ohne Oracle-Installation verwendet. Der Thin-Treiber stellt eine Verbindung mit der Oracle-Datenbank über Java-Sockets her.

   oci

   Der Treibertyp "OCI" wird auf der Client-Seite mit Oracle-Installation verwendet. OCI-Treiber verwenden Oracle Call Interface (OCI) für Interaktionen mit der Oracle-Datenbank.

   kprb

   Der Treibertyp "KPRB" wird zum Schreiben von in der Java-Datenbank gespeicherten Vorgängen und Auslösern verwendet.

4. Akzeptieren Sie die standardmäßige Treibereingabe (oracle.jdbc.OracleDriver), oder ändern Sie die Treibereingabe.
5. Geben Sie Speicherort und Anmeldeinformationen des Oracle-Servers ein:
   a. Geben Sie den Host an, auf dem die Oracle-Datenbank ausgeführt wird.
   b. Geben Sie den Standardport für die Oracle-Datenbank an.
   c. Geben Sie den Standardanwendernamen für den Oracle-Datenbankanwender an.
   d. Geben Sie das Kennwort an, das mit dem angegebenen Anwendernamen verbunden ist.

6. Geben Sie die ID des Oracle-Services an.
7. Geben Sie die Quelle der Inhalte von "tnsnames.ora" im Oracle-Verzeichnis an.

   Die Datei "Oracle TNS Names" übersetzt einen lokalen Datenbankalias in Informationen, die die Konnektivität zur Datenbank aktivieren. Diese Informationen enthalten die IP-Adresse, den Port und die Datenbankdienst-ID.
8. Akzeptieren Sie die standardmäßige maximale Anzahl abzurufender Zeilen (10), oder wählen Sie einen Wert bis 512 aus.
9. Geben Sie die standardmäßige Methode für Datenverschlüsselung ein. Erwägen Sie, einen der folgenden Werte einzugeben, wobei RCA_128 und RCA_256 nur für Heimanwendungen geeignet sind:
   - RC4_40
   - RC4_56
   - RC4_128
   - RC4_256
   - DES40C
   - DES56C
   - 3DES112
   - 3DES168
   - SSL
   - AES128
   - AES256
   - AES192
10. Geben Sie den Standard der Prüfsummen ein, die Oracle unterstützt. Weitere Informationen finden Sie in Ihrer Oracle-Dokumentation.
11. Klicken Sie auf Speichern und Schließen.
12. Klicken Sie auf "Speichern".
13. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren von Datenbanken: Standardmäßige MSSQL-Eigenschaften

Sie können die Operatoren-Kategorie "Datenbanken" für MS SQL Server konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Datenbanken, und wählen Sie Bearbeiten aus.
3. Klicken Sie auf die Registerkarte "Standardmäßige MSSQL-Eigenschaften".
4. Akzeptieren Sie "com.microsoft.sqlserver.jdbc.SQLServerDriver " als Standardtreiber für MSSQL Server.
5. Geben Sie den Hostnamen oder IP-Adresse des Hosts ein, auf dem MSSQL Server ausgeführt wird, um sie als Standardwerte zu verwenden.
6. Gibt den Standardport für MSSQL Server an (üblicherweise 1433).
7. Geben Sie Standardanmeldeinformationen für den MSSQL-Datenbankanwender an.
   - Geben Sie einen Anwendernamen ein.
   - Geben Sie das Kennwort an, das mit dem angegebenen Anwendernamen verbunden ist.
8. Akzeptieren Sie die standardmäßige maximale Anzahl abzurufender Zeilen (10), oder wählen Sie einen Wert bis 512 aus.
9. Geben Sie den Standardnamen der MSSQL-Datenbank ein.
10. Geben Sie den Standardnamen der MSSQL-Instanz ein.
11. Klicken Sie auf Speichern und Schließen.
12. Klicken Sie auf "Speichern".
13. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Aktivieren von "Integrierte Sicherheit von Windows" für das JDBC-Modul für MSSQL Server

Sie können es Operatoren in der Kategorie "Datenbanken" für Microsoft SQL Server (MSSQL) ermöglichen, integrierte Sicherheit zu verwenden. Diese Operatoren können integrierte Sicherheit verwenden, wenn mit Kontaktpunkten auf Hosts, die unter Windows-Betriebssystemen ausgeführt werden, eine Verbindung hergestellt wird.

Ein Datenbankoperator ist ein Operator in der Kategorie "Datenbanken". Zielhosts sind Hosts mit einem Agenten oder Koordinationsrechner. Kopieren Sie für jeden Zielhost, auf den ein Datenbankoperator zugreifen kann, "sqljdbc_auth.dll" in den Systempfad dieses Hosts. Dieser Prozess konfiguriert die Kategorie "Datenbanken" für MSSQL, damit sie integrierte Sicherheit mit Windows-Authentifizierung verwendet.

Sie können die integrierte Sicherheit von Windows für die Kategorie "Datenbanken" für MSSQL Server aktivieren.

Gehen Sie folgendermaßen vor:

1. Wenn Sie die Version des Microsoft SQL Server-Treibers verwenden, die mit CA Process Automation verpackt ist, laden Sie die Version 3.0 des Treibers von der Microsoft-Website herunter. Suchen Sie anderenfalls die vollständige Treiberversion (oder laden Sie sie erneut herunter).
2. Suchen Sie die verpackte oder heruntergeladene Datei "sqljdbc_auth.dll", die der Hardware entspricht, auf der der Agent oder der Koordinationsrechner ausgeführt wird.

3. Kopieren Sie die Datei "sqljdbc_auth.dll" in einen Ordner im Systempfad von jedem CA Process Automation-Agenten oder -Koordinationsrechner, der in einer Windows-Betriebsumgebung ausgeführt wird.

   Um den Systempfad zu bestimmen, führen Sie *eine* der folgenden Aktionen aus:

   - Geben Sie in der Eingabeaufforderung folgenden Befehl ein:

     echo %PATH%

     Der Systempfad wird angezeigt.

   - Gehen Sie zu "Start", "Einstellungen", "Systemsteuerung", "System", "Erweitert" (Erweiterte Systemeinstellungen), "Umgebungsvariablen". Der Systempfad wird in der PATH-Variablen angezeigt.

4. Starten Sie den Agenten oder Koordinationsrechner neu.

Hinweise:

- Wenn Sie eine Verbindungs-URL ohne integrierte Sicherheit erstellen, geben Sie den Anwendernamen und das Kennwort an. Um integrierte Sicherheit zu verwenden, geben Sie den Anwendernamen und das Kennwort nicht an.
- Hängen Sie ";integratedSecurity=true" an die Verbindungs-URL an. Zum Beispiel:

  ```
  jdbc:sqlserver://localhost ... ;integratedSecurity=true
  ```

Konfigurieren von Datenbanken: Standardmäßige MySQL-Eigenschaften

Sie können die Operatoren-Kategorie "Datenbanken" für My SQL Server konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Datenbanken, und wählen Sie Bearbeiten aus.
3. Klicken Sie auf die Registerkarte "Standardmäßige MySQL-Eigenschaften".
4. Akzeptieren Sie "com.mysql.jdbc.Driver" als Standardtreiber für MySQL.
5. Identifizieren Sie den Host, auf dem die MySQL-Datenbank ausgeführt wird.
6. Geben Sie den Standardport der MySQL-Datenbank ein, zum Beispiel 3306.
7. Geben Sie die Standardanmeldeinformationen für die standardmäßige MySQL-Datenbank ein.

   a. Geben Sie den Standardanwendernamen für den MySQL-Datenbankanwender an.

   b. Geben Sie das Kennwort an, das mit dem angegebenen Anwendernamen verbunden ist.

8. Akzeptieren Sie die standardmäßige maximale Anzahl abzurufender Zeilen (10), oder wählen Sie einen Wert bis 512 aus.
9. Geben Sie den Standardnamen der MySQL-Datenbank ein.
10. Klicken Sie auf Speichern und Schließen.
11. Klicken Sie auf "Speichern".
12. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren von Datenbanken: Standardmäßige Sybase-Eigenschaften

Sie können die Operatoren-Kategorie "Datenbanken" für Sybase konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Datenbanken, und wählen Sie Bearbeiten aus.
3. Klicken Sie auf die Registerkarte "Standardmäßige Sybase-Eigenschaften".
4. Wählen Sie einen der folgenden Werte für das standardmäßige relationale Sybase-Datenbanksystem aus:
   - Adaptive Server Anywhere (ASA)
   - Adaptive Server Enterprise (ASE)
5. Akzeptieren Sie "Tds", oder geben Sie ein anderes Standardverbindungsprotokoll ein.
6. Akzeptieren Sie "com.sybase.jdbc2.jdbc.SybDriver", oder geben Sie einen anderen Standardtreiber ein.
7. Geben Sie den Speicherort der Sybase-Datenbank an.
   a. Identifizieren Sie den Serverhost.
   b. Geben Sie den Standardport ein.
8. Geben Sie die Standardanmeldeinformationen für die standardmäßige Sybase-Datenbank ein.
   a. Geben Sie den standardmäßigen Anwendernamen ein.
   b. Geben Sie das Kennwort an, das mit dem angegebenen Anwendernamen verbunden ist.

9. Akzeptieren Sie 10 als die standardmäßige maximale Anzahl abzurufender Zeilen, oder wählen Sie einen Wert bis 512 aus.
10. Geben Sie die Größe des Speichers an, den der Treiber verwendet, um nicht empfindliche Ergebnissatzdaten in einer der folgenden Weisen zwischenzuspeichern:

    -1

    Alle Daten werden zwischengespeichert.

    0

    Bis zu 2 GB Daten werden zwischengespeichert.

    n

    Gibt die Puffergröße in KB an, wobei der Wert eine Potenz von 2 sein muss (eine gerade Zahl). Wenn das angegebene Limit erreicht wird, werden die Daten zwischengespeichert.
11. Geben Sie an, ob Sie den JDBC v3.0-konformen Mechanismus als standardmäßige Umgehungslösung für Massenprozesse verwenden wollen.

    Hinweis: Wenn keine Angabe getroffen wird, wird der systemeigene Mechanismus für Massenprozesse verwendet.
12. Klicken Sie auf Speichern und Schließen.
13. Klicken Sie auf "Speichern".
14. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Über Date-Time

Operatoren in der Kategorie "Datum - Uhrzeit" können auf Koordinationsrechnern ausgeführt werden. Die Kategorie "Datum - Uhrzeit" unterstützt Datums- und Zeitoptionen für Operatoren in anderen Kategorien und bedingte Operatoren für die Ausführung von Verzweigungen in einem Prozess. Einige Beispiele:

- Vergleichen des aktuellen Datums und der aktuellen Uhrzeit mit einem angegebenen Datum und einer angegebenen Uhrzeit.
- Testen, ob sich das aktuelle Datum innerhalb einer Kalenderregel befindet.
- Warten auf ein angegebenes Datum und eine angegebene Uhrzeit.

Die Kategorie "Datum - Uhrzeit" von Operatoren besitzt keine konfigurierbaren Eigenschaften.

Informationen zum Directory-Service

Die Operatoren-Kategorie "Directory-Service" gibt eine Schnittstelle an, um das Lightweight Directory Access Protocol (LDAP) zu unterstützen. Die Directory-Service-Operatoren können auf einem Koordinationsrechner oder Agenten ausgeführt werden.

Konfigurieren von Verzeichnisdienst-Standards

Sie können Verzeichnisdienste konfigurieren. Die Operatorkategorie "Verzeichnisdienste" gibt eine Schnittstelle an, die LDAP/AD unterstützt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Verzeichnisdienste, und wählen Sie Bearbeiten aus.
3. Geben Sie eine Standardanzahl für die Massenrückgabe von Ergebnissen von Betriebsabläufen an, um dabei zu helfen, Leistung und Ressourcenauslastung des Servers zu optimieren. Wählen Sie einen Wert zwischen 1 und 1000 aus, oder geben Sie 0 ein, damit der Server die Anzahl bestimmt.
4. Wählen Sie einen Wert für die Höchstanzahl von Objekten an, die zurückgegeben werden, wenn die Operatoren "Objekt abrufen" oder "Anwender abrufen" ausgeführt werden.
5. Geben Sie die folgenden Factory-Klassennamen an:
   a. Akzeptieren Sie den Standard, com.sun.jndi.ldap.LdapCtxFactory als den vollqualifizierten Klassennamen der Factory-Klasse, die einen anfänglichen Kontext erstellt.
   b. Geben Sie eine durch Doppelpunkte getrennte Liste mit vollqualifizierten Klassennamen von Zustands-Factory-Klassen an, die den Zustand von einem angegebenen Objekt abrufen können. Lassen Sie dieses Feld leer, um die standardmäßigen Zustands-Factory-Klassen zu verwenden.
   c. Geben Sie eine durch Doppelpunkte getrennte Liste mit vollqualifizierten Klassennamen von Factory-Klassen an, mit der ein Objekt aus den Informationen zum Objekt erstellt wird. Lassen Sie dieses Feld leer, um die standardmäßigen Objekt-Factory-Klassen zu verwenden.
6. Geben Sie eine durch Doppelpunkte getrennte Liste mit Sprach-Tags an, in der Tags in RFC 1766 definiert sind. Lassen Sie dieses Feld leer, um den LDAP-Server die Sprachvoreinstellung bestimmen zu lassen.

7. Wählen Sie einen der folgenden Werte aus, um anzugeben, wie der LDAP-Server Empfehlungen verarbeiten soll.

   Ignore

   Ignoriert die Empfehlungen.

   Follow

   Folgt den Empfehlungen.

   Throw

   Gibt die erste Empfehlung zurück, die der Server findet, und die Suche wird angehalten.

8. Geben Sie den Authentifizierungsmechanismus, den der LDAP-Server verwendet, durch eine der folgenden Eingaben an:

   Keine

   Es wird keine Authentifizierung (anonym) verwendet.

   Einfach

   Schwache Authentifizierung verwenden (Klartextkennwort). Wählen Sie diese Option aus, wenn Sie "Sicherheitsprotokoll" auf "SSL" festlegen.

   Space-separated SASL mechanism list

   Ermöglicht es LDAP, einen beliebigen Authentifizierungstyp zu unterstützen, der zwischen LDAP-Client und Server vereinbart wird.

9. Geben Sie das Sicherheitsprotokoll auf eine der folgenden Weisen an:

   - Geben Sie **ssl** ein, um das Protokoll anzugeben, das LDAP-Serververbindungen über ein sicheres Socket zulässt.

     Wichtig! Wenn Sie mit Active Directory (AD) Verbindung aufnehmen, geben Sie **ssl** in *Kleinbuchstaben* ein. AD lehnt den Wert "SSL" ab.

   - Lassen Sie den Wert leer, um Basiskonnektivität zu verwenden.

10. Wählen Sie einen Wert aus, um den Zeitlimit-Wert für die Verbindung anzugeben, oder geben Sie 0 (Null) ein, um keine Zeitüberschreitung festzulegen.

11. Geben Sie den Standort des Standard-LDAP-Servers und die standardmäßigen Anmeldeinformationen ein.

    a. Geben Sie den Hostnamen oder die IP-Adresse ein.

    b. Geben Sie den Standardport für den LDAP-Server an. Ziehen Sie die folgenden Ports in Erwägung:

       - 389: Der ldap-Port für Lightweight Directory Access Protocol (LDAP).
       - 636: Der ldaps-Port für das ldap-Protokoll über TLS/SSL.

   c. Geben Sie die Anwender-ID des standardmäßigen LDAP-Anwenders ein. Operatoren können diesen Standard verwenden oder überschreiben.
   d. Geben Sie das Standardkennwort für den LDAP-Anwender ein. Operatoren können diesen Standard verwenden oder überschreiben.

12. Geben Sie den standardmäßigen Basis-DN (Distinguished Name) an. Operatoren können diesen Standard verwenden oder überschreiben.
13. Geben Sie entweder **uid** oder **cn** als standardmäßiges Anwenderpräfix ein.
14. Klicken Sie auf Speichern und Schließen.
15. Klicken Sie auf "Speichern".
16. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Informationen zu E-Mail

Die Operatorkategorie "E-Mail" ermöglicht es Ihnen, mit Meldungen und Ordnern auf einem E-Mail-Server zu arbeiten. E-Mail-Operatoren kommunizieren mit Ihrem Mail-Server bei der entfernten Verwendung von einem der folgenden Protokolle:

- Post Office Protocol - Version 3 (POP3)
- POP3-SSL
- Internet Message Access Protocol (IMAP)
- IMAP-SSL

Einige Operatoren, wie z. B. jene Operatoren, die Ordner bearbeiten, werden nur dann unterstützt, wenn das IMAP-Protokoll verwendet wird.

Hinweis: Weitere Informationen zum Protokoll, das jeder E-Mail-Operator unterstützt, finden Sie im *Referenzhandbuch für Inhaltsdesign*.

Konfigurieren von standardmäßigen E-Mail-Eigenschaften

Sie können Standardeinstellungen für E-Mail-Operatoren konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf E-Mail, und wählen Sie Bearbeiten aus.

3. Geben Sie den Hostnamen des SMTP-Servers für Java-E-Mail-Alarme ein.
4. Geben Sie die E-Mail-Adresse an, die im Absenderfeld von ausgehenden Java-E-Mail-Alarmen angezeigt wird. Konfigurieren Sie dieses Konto vollständig. Zum Beispiel:

   `anwendername@firmenname.com`

5. Wählen Sie das Standardprotokoll aus, das verwendet wird, um E-Mails von einem Remote-Server oder Remote-Webserver zu empfangen.
   - IMAP
   - POP3
   - IMAP-SSL
   - POP3-SSL
6. Identifizieren Sie den standardmäßigen Mailserver, von dem die E-Mail abgerufen wird.
7. Geben Sie den Standardport des standardmäßigen Mailservers für eingehende E-Mails ein. Ziehen Sie die folgenden Ports in Erwägung:

   143

   Der IMAP-Port für eine ungesicherte Verbindung.

   110

   Der POP3-Port für eine ungesicherte Verbindung.

   993

   Der IMAP-SSL-Port für gesicherte Verbindung.

   995

   Der POP3-SSL-Port für gesicherte Verbindung.

8. Geben Sie standardmäßige Anmeldeinformationen für den E-Mail-Anwender folgendermaßen ein, oder lassen Sie den Wert leer, wenn er immer auf Operatorebene angegeben wird.
   a. Geben Sie einen Anwendernamen ein.
   b. Geben Sie das dazugehörige Kennwort ein.
9. Klicken Sie auf Speichern und Schließen.
10. Klicken Sie auf "Speichern".
11. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Info zum Dateimanagement

Die Dateimanagement-Kategorie von Operatoren kann entweder auf einem Agenten oder auf einem Koordinationsrechner ausgeführt werden. Dateimanagement-Operatoren überwachen die Existenz oder den Status einer Datei oder eines Verzeichnisses. Dateimanagement-Operatoren suchen zusätzlich nach bestimmten Mustern innerhalb des Inhalts einer Datei. POSIX-Regeln bestimmen die Muster der Textmusterübereinstimmung. Diese Funktion kann verwendet werden, um die Weiterverarbeitung in einem Prozess zu bestimmen. Die Dateimanagement-Operatoren können zum Beispiel auf eine XML-Datei warten, die zu verarbeitende Muster enthält. Das Dateimanagement kann Fehlermeldungen in den Inhalten von Protokolldateien suchen.

Die Dateimanagement-Kategorie von Operatoren sucht nach Dateien oder überwacht die Inhalte einer Datei auf dem Ziel. Die Dateien können sich auf einem anderen Computer oder Netzlaufwerk befinden, aber sie müssen für die Operatoren sichtbar sein. Alle Dateimanagement-Operatoren (wie das Erstellen von Verzeichnispfaden und das Prüfen von Dateiinhalten) werden als Administrator oder als der Anwender ausgeführt, der den Kontaktpunkt gestartet hat.

Die speziellen Bedingungen zum Testen oder Warten umfassen:

- das Aussehen einer Datei
- das Fehlen einer Datei
- Bedingungen zur Größe einer Datei
- Datum und Uhrzeit der letzten Änderung
- Das Vorhandensein einer Zeichenfolge oder eines Musters in einer Datei (basierend auf POSIX-Masken)

Konfigurieren des Dateimanagements

Sie können Standardeinstellungen für Operatoren in der Kategorie "Dateimanagement" konfigurieren. Falls nicht anders angegeben, beziehen sich die referenzierten Felder auf UNIX- oder Linux-Betriebssysteme und auch auf Microsoft Windows-Betriebssysteme.

Hinweis: Um ein Feld für eine Eingabe im Fenster "Dateimanagement", die länger ist als der angegebene Speicherplatz, zu erweitern, klicken Sie mit der rechten Maustaste auf das Feld, und wählen Sie dann "Expandieren" aus.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Dateimanagement, und wählen Sie Bearbeiten aus.

3. Führen Sie folgende Schritte im Fenster "Dateimanagement" durch:

   a. Klicken Sie entsprechend für das Betriebssystem, das Sie konfigurieren, auf "Standardmäßige Eigenschaften der Windows-Dateiverwaltung" oder "Standardmäßige Eigenschaften der UNIX-Dateiverwaltung".

   b. Füllen Sie folgende Felder aus, wenn Sie das Feld "Anmeldeinformationen anfordern" auf "Standardmäßig der unten angegebene Anwender" festlegen:

      - Anwender
      - Kennwort
      - Kennwort bestätigen

   c. (UNIX) Definieren der System-Shell des Operators. Geben Sie zum Beispiel einen der folgenden Werte für Shell ein:

      - /bin/bash
      - /bin/csh/
      - /bin/ksh

   d. (UNIX) Aktivieren oder deaktivieren Sie das Kontrollkästchen "Kennwortüberprüfung deaktivieren", je nachdem, ob das Produkt das Anwenderkennwort überprüfen soll, wenn der Anwender gewechselt wird.

   e. Geben Sie den Befehl ein, der eine Datei oder ein Verzeichnis im Feld "Hilfsprogramm zur Komprimierung" komprimiert. Zum Beispiel:

      ```
      WZZIP -P -r {0} {1}
      ```

      ```
      gzip -qrf {0}
      ```

      - {0} ist der Name der komprimierten Ausgabedatei.
      - {1} ist der Name der Quelldatei, die komprimiert werden soll.

   f. Geben Sie den Befehl ein, der eine komprimierte Datei oder ein komprimiertes Verzeichnis im Feld "Hilfsprogramm dekomprimieren" extrahiert. Zum Beispiel:

      ```
      WZUNZIP -d -o -yO {0}
      ```

      ```
      gunzip -qrf {0}
      ```

      {0} ist der Name der komprimierten Datei, die extrahiert werden soll.

4. Klicken Sie auf Speichern und Schließen.

5. Klicken Sie auf "Speichern".

6. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Info zur Dateiübertragung

Die Dateiübertragungskategorie agiert als FTP-Client (File Transfer Protocol), der Remote-Datei-Operatoren in einem Prozess unterstützt. Operatoren in der Dateiübertragungskategorie können entweder auf Koordinationsrechner oder auf Agentenkontaktpunkten ausgeführt werden. Die Kategorie "Dateitransfer" unterstützt alle Befehle, die vom standardmäßigen FTP unterstützt werden, einschließlich:

- Dateiübertragungen an/von einem Remote-Host, der FTP unterstützt.
- Abrufen von Datei-/Verzeichnisinformation von einem Remote-Host.
- Löschen einer Datei/eines Verzeichnisses.
- Umbenennen einer Datei/eines Verzeichnis.

Für FTP-basierte Operatoren, die standardmäßiges FTP und standardmäßige FTP-Server verwenden, sind keine Voraussetzungen erforderlich. Verwenden Sie für SFTP-Übertragungen SSH2, und bereiten Sie den Kontaktpunkt für die Kommunikation mit dem SFTP-Servercomputer basierend auf den aus Anwendername und Kennwort bestehenden Anmeldeinformationen vor.

Stellen Sie eine SSH-Verbindung her, und richten Sie die Zertifikate mit einem SSH-Client ein, bevor Sie SFTP verwenden. CA Technologies stellt einen Test-SSH-Client für Windows bereit, sodass Sie diese erste Verbindung herstellen können. Die meisten UNIX-Computer verfügen bereits über diese Verbindung. Der Vorteil von SFTP ist, dass es sicher ist. Mit SFTP gehen Daten durch einen verschlüsselten Tunnel, und Kennwörter werden authentifiziert.

Konfigurieren des Dateitransfers

Sie können standardmäßige Einstellungen für alle Operatoren in der Kategorie "Dateitransfer" konfigurieren. In allen Fällen können die von Ihnen konfigurierten Werte auf Operatorebene überschrieben werden. Weitere Informationen finden Sie im Abschnitt "Kategorienkonfiguration und Operatorvererbung (siehe Seite 326)".

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Dateitransfer, und wählen Sie Bearbeiten aus.
3. Füllen Sie im Fenster "Dateitransfer" das Feld "Standardmäßiger UDP-Port für Trivial FTP" (Port 69 ist der normale Wert) aus.
4. Klicken Sie auf Speichern und Schließen.
5. Klicken Sie auf "Speichern".
6. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Weitere Informationen:

Überschreiben übernommener Einstellungen einer Kategorie von Operatoren (siehe Seite 330)

Informationen über die Java-Verwaltung

Java-Verwaltungs-Operatoren können entweder auf einem Agenten oder auf einem Koordinationsrechner ausgeführt werden. Diese Operatoren führen mithilfe der JMX-Technologie (Java Management Extensions) verschiedene Aufgaben auf ManagedBeans-Ressourcen (MBeans) aus. Die Operatoren verwenden einen angegebenen Anwendernamen und ein Kennwort, um eine Verbindung zu einer JMX-Dienst-URL oder einem JMX-Server auf einem angegebenen Host und Port herzustellen.

Bestimmte Operatoren führen die folgenden Aufgaben aus:

- Abrufen von MBeans-Attributen.
- Aufrufen von MBeans-Methoden mithilfe von angegebenen Parametern.
- Festlegen von MBeans-Attributwerten.

Die Kategorie "Java-Verwaltung" besitzt keine konfigurierbaren Eigenschaften.

Info zu Netzwerk-Hilfsprogrammen

Operatoren in der Netzwerk-Hilfsprogramme-Kategorie können sowohl auf Koordinationsrechnern als auch auf Agenten ausgeführt werden und können mit SNMP-Geräten oder SNMP-Managern interagieren (z. B. mit Netzwerkmanagern). Netzwerkhilfsprogramme-Operatoren bestimmen den Zustand eines Konfigurationselements eines IP-Geräts.

Netzwerkhilfsprogramme-Operatoren generieren SNMP-basierte Alarme (Traps) zu Geräten oder zu Netzwerkmanagern. Netzwerkhilfsprogramme wurden entworfen, um einen Prozess zu beeinflussen, nicht um einen vollwertigen Netzwerkmonitor zu implementieren.

Anwender können Operatoren von Netzwerk-Hilfsprogrammen zu folgenden Zwecken aufrufen:

- Abrufen des Wertes von Remote-MIB-Variablen (Management Information Base) und Verwendung ihre Werte im Prozess (zum Beispiel als Parameter oder Bedingungen).
- Warten auf Bedingungen für den Wert von Remote-MIB-Variablen.
- Festlegen von Remote-MIB-Variablen, um das Verhalten von externen Geräten zu beeinflussen.
- Senden von SNMP-Traps, um Fehler und besondere Bedingungen an die SNMP-Verwaltungsplattformen zu melden (zum Beispiel Tivoli, HP OpenView oder ISM).

Netzwerkhilfsprogramme-Operatoren sind verfügbar auf Hosts mit UNIX- und Windows-Betriebssystemen. Netzwerk-Hilfsprogramme identifizieren entfernte MIB-Variablen durch ihre Objekt-IDs (OIDs).

Konfigurieren von Netzwerkhilfsprogrammen

Sie können die Kategorie "Netzwerkhilfsprogramme" von Operatoren konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Dateitransfer, und wählen Sie Bearbeiten aus.
3. Klicken Sie mit der rechten Maustaste auf "Netzwerkhilfsprogramme", und wählen Sie "Bearbeiten" aus.
4. Geben Sie im Feld "Abfragefrequenz (Sek.)" an, wie oft ein Netzwerkhilfsprogramm-Operator synchron die Geräteobjekt-ID (SNMP OID) für eine SNMP-Variable empfängt.

5. Klicken Sie auf Speichern und Schließen.

6. Klicken Sie auf "Speichern".

   Der Konfigurationsvorgang wendet die Änderungen auf Modulebene auf die Produktkonfiguration an.

7. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Info zur Prozesssteuerung

Operatoren in der Kategorie "Prozesssteuerung" können nur auf Koordinationsrechner-Kontaktpunkten ausgeführt werden. Prozesssteuerungs-Operatoren haben die folgenden Funktionen:

- Starten und Interpretieren von CA Process Automation-Prozessen
- Aufrufen anderer Kategorien, um Operatoren in einer Prozessobjektinstanz auszuführen
- Durchsetzen von Abhängigkeiten
- Überwachen von Aufrufen von Kategorien und Festlegen, wie weitere Prozessverzweigungen basierend auf den Aufrufergebnissen ausgeführt werden

Wenn ein Prozess startet, stellt das Produkt eine Kopie (Instanz) aus dem Prozess her. Änderungen an der Kopie wirken sich nicht auf andere Kopien oder den ursprünglichen Prozess aus. Sie können einen Prozess auf eine der folgenden Weisen starten:

- Mit dem Formulardesigner.
- Durch einen Ablaufplan.
- Durch einen anderen Prozess.
- Durch eine externe Anwendung, die einen CA Process Automation-Auslöser verwendet.
- Durch eine externe Anwendung, die SOAP-Aufrufe verwendet. Informationen finden Sie im *Webservice-API-Referenzhandbuch*.

Bei stark dezentralisierten Architekturen sollten Sie logische Gruppen von Operatorkategorien in einer Umgebung definieren und die Prozesssteuerung auf einem ausgewählten Kontaktpunkt in den einzelnen Gruppen konfigurieren. In einer solchen Konfiguration startet das Produkt Prozesse auf dem Kontaktpunkt, auf dem die Prozesssteuerungs-Operatoren für eine Gruppe ausgeführt werden. Sie konfigurieren einen Kontaktpunkt speziell für das Ausführen von Prozessen mit mehreren Gruppen. Beim Ausführen der Prozesse hat eine dezentralisierte Architektur die folgenden Vorteile:

- Sie reduziert die Ladung auf den einzelnen Computern
- Sie reduziert die Auswirkung von potenziellen Incidents
- Sie reduziert die Datenmenge, die auf Remote-Hosts ausgetauscht wird

Konfigurieren der Prozesssteuerung

Sie können die Standardeinstellung für Operatoren in der Prozesssteuerungs-Kategorie konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Prozesssteuerung, und wählen Sie Bearbeiten aus.
3. Füllen Sie im Fenster "Prozesssteuerung" das Feld "Zeit, während der abgeschlossene Anwenderinteraktionen aufbewahrt werden (Min.)" aus.
4. Klicken Sie auf Speichern und Schließen.
5. Klicken Sie auf "Speichern".
6. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Informationen zu Hilfsprogrammen

Die Kategorie "Hilfsprogramme" auf der Registerkarte "Module" enthält Felder, die zum Operator "Java aufrufen" gehören.

Wichtig! Der Operator "Java aufrufen" wird nur auf einem Agenten ausgeführt und kann nicht für einen Koordinationsrechner konfiguriert werden.

Mit der Kategorie "Hilfsprogramme" können Sie Folgendes angeben:

- Pfade zu den externen JAR-Dateien, die standardmäßig für alle "Java aufrufen"-Operatoren geladen werden sollen.
- Standardmäßige Protokollierung.

Jede angegebene JAR-Datei ist für den Java-Code verfügbar, der durch die "Java aufrufen"-Operatoren ausgeführt wird. Die Klassen, die auf Operatorebene in JAR-Dateien definiert sind, überschreiben die gleichen Klassen, die in den JAR-Dateien für die Kategorie "Hilfsprogramme" angegeben sind.

Bei entsprechender Konfiguration können Designer die Protokollierung im Kontext des Codes verwenden. Zum Beispiel:

```
logger.debug()
logger.info()
```

Sie können die Protokollierung so konfigurieren, dass die protokollierten Daten keine Informationen enthalten.

Konfigurieren von Hilfsprogrammen

Sie können Standardeinstellungen für den Operator "Java aufrufen" in der Kategorie "Hilfsprogramme" nur dann konfigurieren, wenn der Operator auf einem Agenten ausgeführt wird. Anderenfalls benötigt diese Operatorkategorie keine Konfiguration. Der Operator "Java aufrufen" darf nicht auf Koordinationsrechnern ausgeführt werden.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Hilfsprogramme, und wählen Sie Bearbeiten aus.

   Die Registerkarte "Standardeigenschaften des Operators 'Java aufrufen'" wird geöffnet
3. Aktivieren Sie das Kontrollkästchen "Strict Java Mode verwenden", um eingegebene Variablendeklarationen, Methodenargumente und Rückgabetypen im Code der Hauptmethode zur Laufzeit durchzusetzen.
4. Klicken Sie auf "Parameter hinzufügen" , und definieren Sie entsprechend die externen JAR-Dateien.
5. Um eine ausgewählte JAR-Datei zu entfernen, wählen Sie ein Element aus der Liste "Externe JAR-Dateien" aus, und klicken Sie dann auf "Löschen".
6. Füllen Sie die verbleibenden Felder im Fenster "Hilfsprogramme" entsprechend aus.
7. Klicken Sie auf Speichern und Schließen.
8. Klicken Sie auf "Speichern".
9. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Info zu Webservices

Webservices-Operatoren können sowohl auf Koordinationsrechnern als auch auf Agenten ausgeführt werden. Zwei der Operatoren stellen eine Schnittstelle zu Remote-Diensten bereit, die durch SOAP zur Verfügung gestellt werden. Für diese Operatoren gilt:

- Erstellt eine SOAP-Anfrage.

  Die Daten können zur Laufzeit aus vorhandenen CA Process Automation-Datensätzen und -Variablen oder aus externen Quellen extrahiert werden.

- Sendet die SOAP-Abfrage zur entsprechenden Operatorkategorie "Webservices", die zur Entwurfs- oder zur Laufzeit angegeben wird.
- Ruft gegebenenfalls Fehlerbedingungen für die Antwortverarbeitung ab.
- Analysiert die eingehende Antwort und speichert die Ergebnisse in CA Process Automation-Datensätzen, auf die nachfolgende Operatoren in einem Prozess zugreifen.
- Ein asynchroner Anruf sendet die Anfrage und wartet auf eine Antwort vom Remote-Ziel, nachdem eine Bestätigung empfangen wurde. Asynchrone Anrufe verwenden ein komplexeres Senden und Empfangen als synchrone Anrufe. Nachfolgende Operatoren in einem Prozess greifen auf die zurückgegebenen Daten zu.

Webservices stellen die Möglichkeit bereit, Datenverwaltungseinrichtungen über ein Netzwerk zu automatisieren, das HTTP verwendet. Zum Beispiel können Inhaltsdesigner Prozesse entwickeln, die RESTful-Services über HTTP-Operatoren automatisieren. Wenn ein HTTP-Operator mit einem leeren Feld konfiguriert ist, vererbt dieser Operator den Standardwert des entsprechenden Felds von der übergeordneten Kategorieeinstellung. Daher wird nichts aktiviert oder deaktiviert, wenn Sie eine Auswahl für ein Operatorkategoriefeld vornehmen. Sie können alle Standards nach eigenem Ermessen angeben. Wenn Sie diese gleichen Optionen auf der Operatorebene konfigurieren, deaktiviert die Auswahl einer Option die Auswahl einer anderen Option.

Konfigurieren von Webservices

Sie können Standardeinstellungen für Operatoren in der Webservices-Kategorie konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte Module, klicken Sie mit der rechten Maustaste auf Webservices, und wählen Sie Bearbeiten aus.

3. Klicken Sie auf im Fenster "Webservices" auf "Standardmäßige Webservices-Eigenschaften", und überprüfen oder aktualisieren Sie die Felder entsprechend.
4. Klicken Sie auf "Standardmäßige Webservices-HTTP-Eigenschaften", und überprüfen oder aktualisieren Sie die Felder entsprechend.
5. Klicken Sie auf Speichern und Schließen.
6. Klicken Sie auf "Speichern".
7. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren von Werten für eine anwenderspezifische Operatorgruppe

Sie können Werte für Variablen konfigurieren, die Sie für eine ausgewählte anwenderspezifische Operatorgruppe definiert haben. Anwenderspezifische Operatorgruppen werden auf der Registerkarte "Gruppenkonfiguration" eines anwenderspezifischen Operator-Editors definiert.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte "Module", klicken Sie mit der rechten Maustaste auf eine anwenderspezifische Operatorgruppe, und wählen Sie die Option "Bearbeiten" aus.

   Die ausgewählte anwenderspezifische Operatorgruppe wird geöffnet. Das Produkt zeigt die Seiten und Variablen zunächst ohne Werte an.
3. Fügen Sie für jedes angezeigte Feld oder Array den Wert hinzu, der als Standard verwendet werden soll.

   Die Standardwerte können auf Umgebungsebene und auf Operatorebene überschrieben werden.
4. Klicken Sie auf Speichern und Schließen.
5. Klicken Sie auf "Speichern".
6. Wenn Sie die Konfiguration der Operatorkategorien und der anwenderspezifischen Operatorgruppen auf der Registerkarte "Module" abgeschlossen haben, wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Hinweis: Wenn Sie eine Variable löschen oder die Datentypenvariable ändern, dann werden die Änderungen nicht bei der Domäne oder in den zugeordneten Umgebungen veröffentlicht.

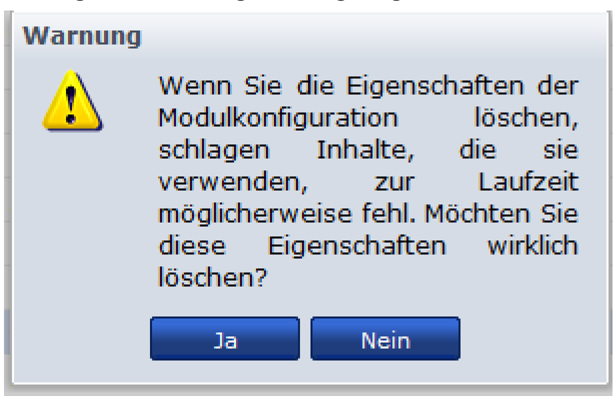
Löschen einer anwenderspezifischen Operatorgruppenkonfiguration

Administratoren können die Registerkarte "Module" im Konfigurationsbrowser verwenden, um die veröffentlichte anwenderspezifische Operatorgruppe aus der Domäne und ihren Umgebungen zu löschen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Klicken Sie mit der rechten Maustaste auf die Domäne, und wählen Sie "Sperren" aus.
3. Klicken Sie mit der rechten Maustaste auf die anwenderspezifische Operatorgruppe, und wählen Sie "Löschen" aus.

   Die folgende Warnung wird angezeigt:

4. Klicken Sie auf "Ja", um den Löschvorgang zu bestätigen.

   CA Process Automation löscht das anwenderspezifische Operatorgruppen-Konfigurationsmodul aus der Domäne. Wenn ein Prozess das anwenderspezifische Operatorgruppen-Konfigurationsmodul verwendet, ist der Prozess fehlerhaft.

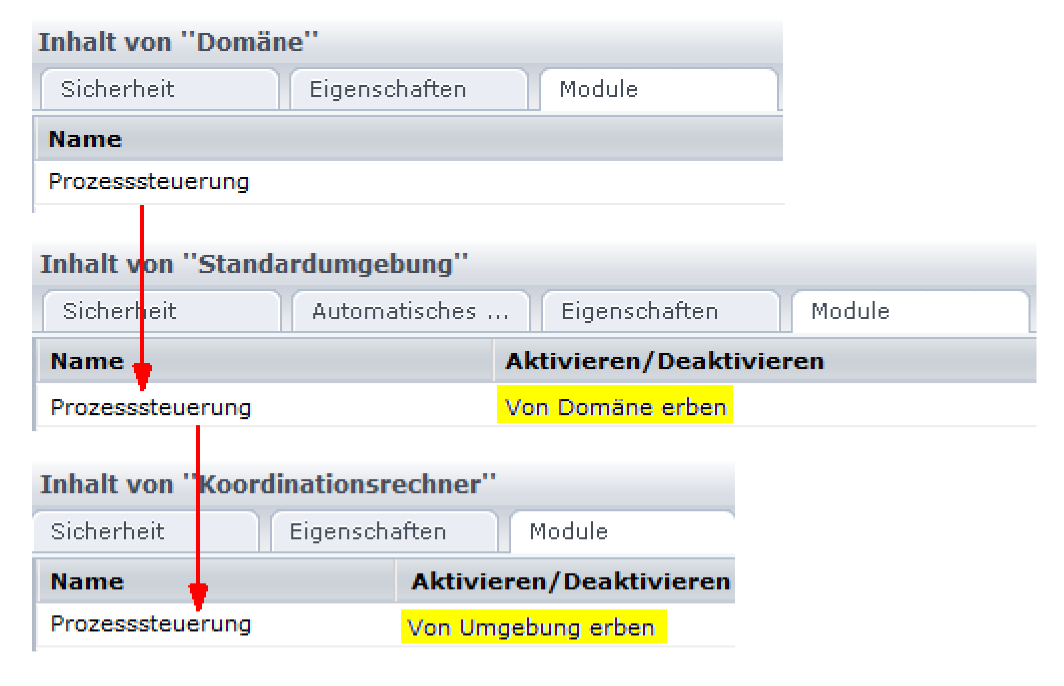
5. Klicken Sie auf "Speichern".

   Die anwenderspezifische Operatorgruppenkonfiguration wird aus der Domäne und ihrer Umgebung gelöscht.

Kategorienkonfiguration und Operatorvererbung

Operatorkategorien, wie "E-Mail" oder "Dateiübertragung", haben konfigurierbare Einstellungen mit vordefinierten Standards. Administratoren können eine Kategorie auf der Registerkarte "Module" auf verschiedenen Ebenen der Domänenhierarchie bearbeiten. Bei der Installation beginnen die Standardeinstellungen für jede Operatorkategorie auf der Domänenebene. Diese Einstellungen werden auf der Umgebungsebene als "Von Domäne übernehmen" markiert. Auf der Ebene des Koordinationsrechners werden diese Einstellungen als "Von Umgebung übernehmen" markiert.

Wie die folgende Abbildung zeigt, werden Einstellungen der Operatorkategorien von der Domäne für jede Umgebung und von jeder Umgebung für Koordinationsrechner in dieser Umgebung übernommen. Sie können Einstellungen auf Domänenebene, auf Umgebungsebene und auf Ebene des Koordinationsrechners überschreiben.



Operatoren für einen Koordinationsrechner übernehmen ihre Einstellungen der Operatorkategorie von diesem Koordinationsrechner. Inhaltsdesigner überschreiben bei Bedarf diese übernommenen Einstellungen auf Operatorebene.

Agenten übernehmen auf Domänenebene konfigurierte Einstellungen, aber Operatoren verwenden diese Einstellungen nicht. Wenn ein Kontaktpunkt einem Agenten zugeordnet ist, schließt die Zuordnung eine Umgebung ein. Zur Laufzeit verwenden Operatoren für einen Kontaktpunkt die Eigenschaften, die für die Umgebung konfiguriert wurden, die dem Kontaktpunkt zugewiesen ist.

Hinweis: Für anwenderspezifische Operatorgruppen, die von einem Anwender definiert wurden, werden Einstellungen von der Domänenebene zur Umgebungsebene übernommen. Administratoren können Einstellungen auf der Umgebungsebene überschreiben, die auf der Domänenebene definiert wurden. Diese Einstellungen sind für das Überschreiben auf Koordinationsrechner- oder Agent-Ebenen nicht verfügbar.

Weitere Informationen:

Operatorkategorien und Operatorordner (siehe Seite 284)

Aktivieren oder Deaktivieren einer Operatorkategorie

Die Einstellungen der Operatorkategorien werden normalerweise auf der Domänenebene konfiguriert. Standardmäßig sind die Einstellungen der Operatorkategorien für Umgebungen auf "Von Domäne übernehmen" festgelegt. Standardmäßig sind die Einstellungen der Operatorkategorien für Koordinationsrechner und Agenten auf "Von Umgebung übernehmen" festgelegt.

Greifen Sie auf die Registerkarte "Module" für eine Umgebung, einen Koordinationsrechner oder einen Agenten zu, um folgende Aktionen durchzuführen:

- Aktivieren einer oder mehrerer Operatorkategorien.
- Deaktivieren einer oder mehrerer Operatorkategorien.
- Konfigurieren einer oder mehrerer aktivierten Kategorien.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".

   Der Konfigurationsbrowser wird geöffnet.

2. Nehmen Sie eine der folgenden Aktionen vor, um eine Sperre auf der gewünschten Ebene zu platzieren:

   - Erweitern Sie den Knoten "Domäne", wählen Sie die Zielumgebung aus, und klicken Sie auf "Sperren".
   - Erweitern Sie den Knoten "Koordinationsrechner", wählen Sie den Ziel-Koordinationsrechner aus, und klicken Sie auf "Sperren".
   - Erweitern Sie den Knoten "Agenten", wählen Sie den Zielagenten aus, und klicken Sie auf "Sperren".

3. Klicken Sie auf die Registerkarte "Module".
4. Wählen Sie eine Operatorkategorie aus, klicken auf die Spalte "Aktivieren/Deaktivieren", und wählen Sie entweder "Aktiviert" oder "Deaktiviert" aus.
5. Klicken Sie auf "Speichern".
6. Klicken Sie auf "Entsperren".

Aktivieren oder Deaktivieren einer anwenderspezifischen Operatorgruppe

Die Einstellungen der anwenderspezifischen Operatorgruppe werden normalerweise auf der Domänenebene konfiguriert. Standardmäßig sind die Einstellungen der anwenderspezifischen Operatorgruppe für Umgebungen auf "Von Domäne übernehmen" festgelegt.

Greifen Sie auf die Registerkarte "Module" für eine Umgebung zu, um folgende Aktionen durchzuführen:

- Aktivieren von einer oder mehreren anwenderspezifischen Operatorgruppen.
- Deaktivieren von einer oder mehreren anwenderspezifischen Operatorgruppen.
- Überschreiben von Einstellungen auf einer oder mehreren aktivierten Gruppen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".

   Der Konfigurationsbrowser wird geöffnet.

2. Erweitern Sie den Knoten "Domäne", wählen Sie die Zielumgebung aus, und klicken Sie auf "Sperren".
3. Klicken Sie auf die Registerkarte "Module".
4. Wählen Sie einen anwenderspezifischen Operator aus, klicken Sie auf die Spalte "Aktivieren/Deaktivieren", und wählen Sie entweder "Aktiviert" oder "Deaktiviert" aus.
5. Klicken Sie auf "Speichern".
6. Klicken Sie auf "Entsperren".

Überschreiben übernommener Einstellungen einer Kategorie von Operatoren

Ein Administrator mit Domänenadministratorrechten konfiguriert Kategorien für Operatoren auf Domänenebene. Ein Administrator mit Umgebungskonfigurations-Administratorrechten kann übernommene Einstellungen auf einer der folgenden Ebenen überschreiben:

- Umgebung
- Koordinationsrechner
- Agent

Einstellungen der Operatorkategorien, die auf Domänenebene konfiguriert wurden, werden als "Von Domäne übernehmen" angezeigt. Diese Einstellung ist in einer Drop-down-Liste, in der andere gültige Optionen "Aktiviert" und "Deaktiviert" sind. Wählen Sie "Aktiviert" aus, um die übernommenen Einstellungen zu bearbeiten. Wählen Sie "Deaktiviert" aus, um Operatoren in der ausgewählten Kategorie zu deaktivieren.

Sie können übernommene Einstellungen für eine beliebige Kategorie von Operatoren auf einer oder auf mehreren Ebenen überschreiben.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. (Optional) Überschreiben Sie ausgewählte Einstellungen auf Umgebungsebene folgendermaßen:
   a. Klicken Sie mit der rechten Maustaste auf die ausgewählte Umgebung, und wählen Sie "Sperren" aus.
   b. Klicken Sie auf die Registerkarte "Module".
   c. Wählen Sie eine Kategorie aus, wählen Sie in der Drop-down-Liste "Aktivieren/Deaktivieren" die Option "Aktiviert" aus.
   d. Klicken Sie mit der rechten Maustaste auf die Kategorie, und wählen Sie "Bearbeiten" aus.

      Die Eigenschaften der ausgewählten Kategorie werden in einer Liste angezeigt, die per Bildlauf durchsucht werden kann.
   e. Ändern Sie eine oder mehrere übernommene Einstellungen.
   f. Klicken Sie auf "Speichern".
   g. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie "Entsperren" aus.

3. (Optional) Überschreiben Sie ausgewählte Einstellungen auf Koordinationsrechnerebene folgendermaßen:

    a. Erweitern Sie "Koordinationsrechner", wählen Sie einen Koordinationsrechner aus, und klicken Sie auf "Sperren".

    b. Klicken Sie auf die Registerkarte "Module".

    c. Wählen Sie eine Kategorie aus, wählen Sie in der Drop-down-Liste "Aktivieren/Deaktivieren" die Option "Aktiviert" aus.

    d. Klicken Sie mit der rechten Maustaste auf die Kategorie, und wählen Sie "Bearbeiten" aus.

       Die Eigenschaften der ausgewählten Kategorie werden in einer Liste angezeigt, die per Bildlauf durchsucht werden kann.

    e. Ändern Sie eine oder mehrere übernommene Einstellungen.

    f. Klicken Sie auf "Speichern".

    g. Klicken Sie auf "Entsperren".

4. (Optional) Überschreiben Sie ausgewählte Einstellungen auf Agentenebene folgendermaßen:

    a. Erweitern Sie den Knoten "Agenten", wählen Sie einen Agenten aus, und klicken Sie auf "Sperren".

    b. Klicken Sie auf die Registerkarte "Module".

    c. Wählen Sie eine Kategorie aus, wählen Sie in der Drop-down-Liste "Aktivieren/Deaktivieren" die Option "Aktiviert" aus.

    d. Klicken Sie mit der rechten Maustaste auf die Kategorie, und wählen Sie "Bearbeiten" aus.

       Die Eigenschaften der ausgewählten Kategorie werden in einer Liste angezeigt, die per Bildlauf durchsucht werden kann.

    e. Ändern Sie eine oder mehrere übernommene Einstellungen.

    f. Klicken Sie auf "Speichern".

    g. Klicken Sie auf "Entsperren".

Überschreiben geerbter Werte für eine anwenderspezifische Operatorgruppe

Ein Administrator mit Domänenadministratorrechten konfiguriert anwenderspezifische Operatorgruppen auf Domänenebene. Ein Administrator, der über die Rechte eines Umgebungskonfigurations-Administrators verfügt, kann vererbte Einstellungen auf Umgebungsebene überschreiben.

Hinweis: Im Gegensatz zu Operatorkategorien können Sie keine Werte für anwenderspezifische Operatorgruppen auf Koordinationsrechner- oder Agent-Ebene überschreiben.

Einstellungen der anwenderspezifischen Operatorgruppe, die auf Domänenebene konfiguriert wurden, werden als "Von Domäne übernehmen" angezeigt. Diese Einstellung ist in einer Drop-down-Liste, in der andere gültige Optionen "Aktiviert" und "Deaktiviert" sind. Wählen Sie "Aktiviert" aus, um die übernommenen Einstellungen zu bearbeiten. Wählen Sie "Deaktiviert" aus, um anwenderspezifische Operatoren in der ausgewählten Kategorie zu deaktivieren.

Sie können Einstellungen überschreiben, die die ausgewählte Umgebung von der Domäne übernimmt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Klicken Sie mit der rechten Maustaste auf die ausgewählte Umgebung, und wählen Sie dann "Sperren" aus.
3. Klicken Sie auf die Registerkarte "Module".
4. Wählen Sie eine Kategorie aus, wählen Sie in der Drop-down-Liste "Aktivieren/Deaktivieren" die Option "Aktiviert" aus.
5. Klicken Sie mit der rechten Maustaste auf die Kategorie, und wählen Sie dann "Bearbeiten" aus.

   Die Eigenschaften der ausgewählten Kategorie werden in einer Liste angezeigt, die per Bildlauf durchsucht werden kann.
6. Ändern Sie eine oder mehrere übernommene Einstellungen.
7. Klicken Sie auf "Speichern".
8. Klicken Sie mit der rechten Maustaste auf die Umgebung, und wählen Sie dann "Entsperren" aus.

Operatorkategorien und wo Operatoren ausgeführt werden

Einige Operatoren können nur auf Koordinationsrechnern ausgeführt werden, jedoch nicht auf Kontaktpunkten, die Agenten zugeordnet sind. Andere Operatoren werden auf Koordinationsrechnern und Agentenkontaktpunkten ausgeführt, jedoch nicht auf Remote-Hosts, auf die Proxy-Kontaktpunkte oder Hostgruppen verweisen. Mehrere Operatoren können auf einem Zieltyp ausgeführt werden. Einige Operatoren innerhalb einer Operatorkategorie können auf Koordinationsrechnern aber nicht auf Agentenkontaktpunkten ausgeführt werden. Andere Operatoren innerhalb der gleichen Kategorie können sowohl auf Koordinationsrechnern als auch auf Agentenkontaktpunkten ausgeführt werden. Die Möglichkeit zum Ausführen auf einem bestimmten Zieltyp wird nicht fehlerlos zu einer Operatorkategorie zugeordnet.

Hinweis: Unter dem Abschnitt "Wo Operatoren ausgeführt werden können" im *Referenzhandbuch für Inhaltsdesign* finden Sie weitere Informationen zu gültigen Zielen für jeden Operator.

Kapitel 13: Verwalten von Auslösern

Anwendungen, die keine SOAP-Aufrufe vornehmen können, können Auslöser als Alternative verwenden. Die Verwendung von SOAP-Aufrufen wird über Auslöser empfohlen, weil diese Vorgehensweise weniger fehleranfällig ist.

Auslöser ermöglichen externen Anwendungen, einen Prozess in CA Process Automation zu starten. Ein Auslöser ruft den CA Process Automation-Prozess auf, dem in XML-Inhalt oder in einer SNMP-Trap definiert wird. Der XML-Inhalt kann dem konfigurierten Dateispeicherort oder der konfigurierten E-Mail-Adresse bereitgestellt werden. SNMP-Trap-Inhalt wird in einer OID gesendet, die einem konfigurierten regulären Ausdruck entspricht. CA Process Automation sucht nach eingehenden SNMP-Traps auf dem konfigurierten SNMP-Trap-Port (standardmäßig 162).

Dieses Kapitel enthält folgende Themen:

Konfigurieren und Verwenden von Auslösern

Für externe Anwendungen, die keine SOAP-Aufrufe zum Starten von CA Process Automation-Prozessen ausgeben können, stellt CA Process Automation vier vordefinierte Auslöser bereit. Sie können Auslöser konfigurieren, um die Initiierung von Prozessen über eines der folgenden Elemente zu aktivieren:

- Ein Event von einem Catalyst-Connector
- Eine empfangene Datei
- Eine E-Mail
- Ein SNMP-Trap

Nachdem Sie einen Dateiauslöser oder einen E-Mail-Auslöser konfiguriert haben, können Sie XML-Inhalte erstellen. Die XML-Inhalte starten konfigurierte CA Process Automation-Prozesse mit Parametern von den externen Anwendungen. Der XML-Inhalt kann in einer Datei abgelegt und ins konfigurierte Verzeichnis platziert oder als E-Mail zum konfigurierten Konto gesendet werden. Der Auslöser ruft den Prozess auf, der im XML-Inhalt angegeben wird, wenn angegebene Kriterien erfüllt werden. Die vom Auslöser aufgerufene Prozessinstanz füllt auch Prozessdatensätze mit den im XML-Inhalt angegebenen Werten auf.

Nachdem Sie einen SNMP-Trap-Auslöser in CA Process Automation konfiguriert haben, können externe Anwendungen SNMP-Traps an CA Process Automation senden. Wenn CA Process Automation ein SNMP-Trap empfängt, die mit Objekt-IDs (OIDs) und dem Nutzdatenwertfilter übereinstimmt, wird der konfigurierte Prozess gestartet. Der Datensatz des ausgelösten Prozesses erhält die Trap-Informationen.

Nachdem Sie ein Catalyst-Event-Abonnement konfiguriert haben, können externe Catalyst-Connectors Events an CA Process Automation senden. Wenn CA Process Automation ein Catalyst-Event erhält, das mit dem Filter übereinstimmt, wird der konfigurierte Prozess mit den Event-Eigenschaften gestartet, die im Prozessdatensatz verfügbar sind.

Im Gegensatz zu den Einstellungen, die die Umgebung von der Domäne standardmäßig übernimmt, werden Auslöser sowohl auf Umgebungsebene als auch auf Koordinationsrechnerebene standardmäßig deaktiviert. Um CA Process Automation-Auslöser zu aktivieren, die auf Domänenebene festgelegt sind, legen Sie Vererbung von der Domäne auf der Umgebungsebene fest. Legen Sie anschließend die Vererbung von der Umgebung auf die Koordinationsrechnerebene fest. Alternativ können Sie übernommene Werte überschreiben und Auslöserwerte auf Umgebungs- und Koordinationsrechnerebene konfigurieren.

Verwenden Sie die folgende Vorgehensweise, um Auslöser zu implementieren:

1. Konfigurieren Sie Auslöser auf Domänenebene. Diese Konfigurationen werden standardmäßig nicht übernommen. Konfigurieren Sie Auslöser nur dann, wenn Sie planen, die Prozessinitiierung von externen Anwendungen und nur für die Auslösertypen zu akzeptieren, die Sie empfangen möchten.

2. Führen Sie auf Umgebungsebene, auf der der Auslöserstatus deaktiviert ist, eine der folgenden Aktionen aus:

   ■ Behalten Sie den Status "Deaktiviert" für nicht anwendbare Auslösertypen bei.

   ■ Ändern Sie für Umgebungen, in denen die Domänenkonfiguration gilt, den Status auf "Von Domäne übernehmen".

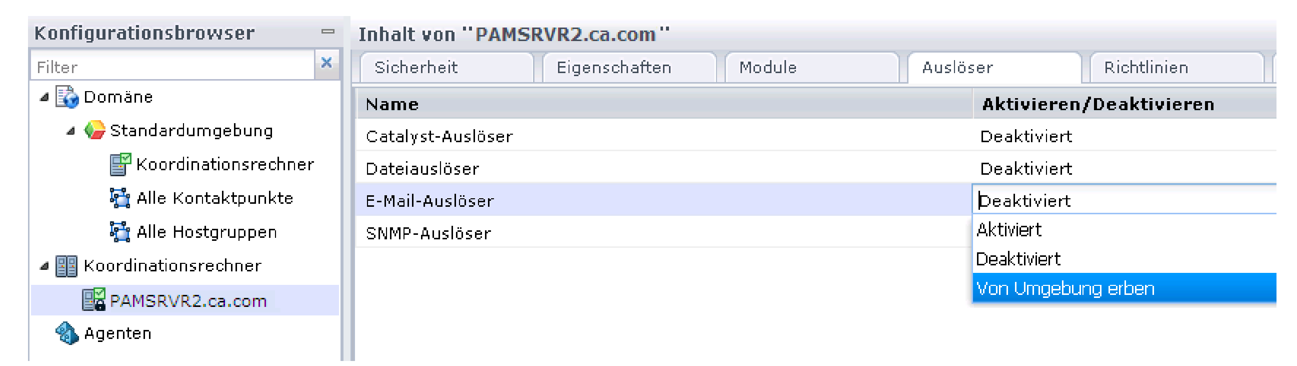


   ■ Ändern Sie den Status auf "Aktiviert", und konfigurieren Sie ggf. die Auslöser auf dieser Ebene.

3. Führen Sie auf Koordinationsrechnerebene, auf der der Auslöserstatus deaktiviert ist, eine der folgenden Aktionen aus:

   ■ Behalten Sie den Status "Deaktiviert" für nicht anwendbare Auslösertypen bei.

   ■ Ändern Sie den Status auf "Von Umgebung übernehmen". Wenn Sie diese Option auswählen, werden Werte zur Laufzeit von der Umgebung übernommen, wenn Auslöser auf Umgebungsebene definiert werden. Andernfalls werden die auf Domänenebene definierten Werte verwendet.



   ■ Ändern Sie den Status auf "Aktiviert", und bearbeiten Sie die Eigenschaften.

4. CA Process Automation durchsucht das konfigurierte Verzeichnis, das konfigurierte E-Mail-Konto und den konfigurierten Port nach Inhalt, der mit den entsprechenden Auslöserkriterien übereinstimmt.

   ■ Externe Anwendungen erstellen die Eingabe für konfigurierte Auslöser:

     – Für einen Dateiauslöser oder E-Mail-Auslöser erstellen sie gültigen XML-Inhalt. XML-Inhalt gibt den Pfad zum startenden Prozess, die Anmeldeinformationen, die Startzeit und die Werte der Initialisierungsparameter an.

     – Für einen SNMP-Trap-Auslöser senden sie eine gültige SNMP-Trap mit Werten, die mit den konfigurierten Kriterien übereinstimmen, an den Port 162.

   ■ Externe Anwendungen senden CA Process Automation-Auslöser als Teil der Automatisierungsverarbeitung.

5. CA Process Automation verarbeitet neuen Inhalt und startet den konfigurierten CA Process Automation-Prozess mit den von der externen Anwendung weitergegebenen Werten.

6. Überwachen Sie die Prozessinstanz, die vom Auslöser, der vom externen Prozess gesendet wurde, aufgerufen wird. Sie können den aktiven Prozess durch Prozessüberwachung überwachen. Sie können die Werte anzeigen, die vom Auslöser auf der Seite mit den Datensatzvariablen für den zugeordneten Auslösertyp weitergegeben werden.

Konfigurieren von Catalyst-Auslösereigenschaften auf Domänenebene

Mit Domänenadministratorrechten können Sie die Eigenschaften "Catalyst-Auslöser" auf der Domänenebene konfigurieren. Mit den vererbten Eigenschaften des Catalyst-Auslösers, kann das Produkt Prozesse starten, wenn ein Catalyst-Event empfangen wird.

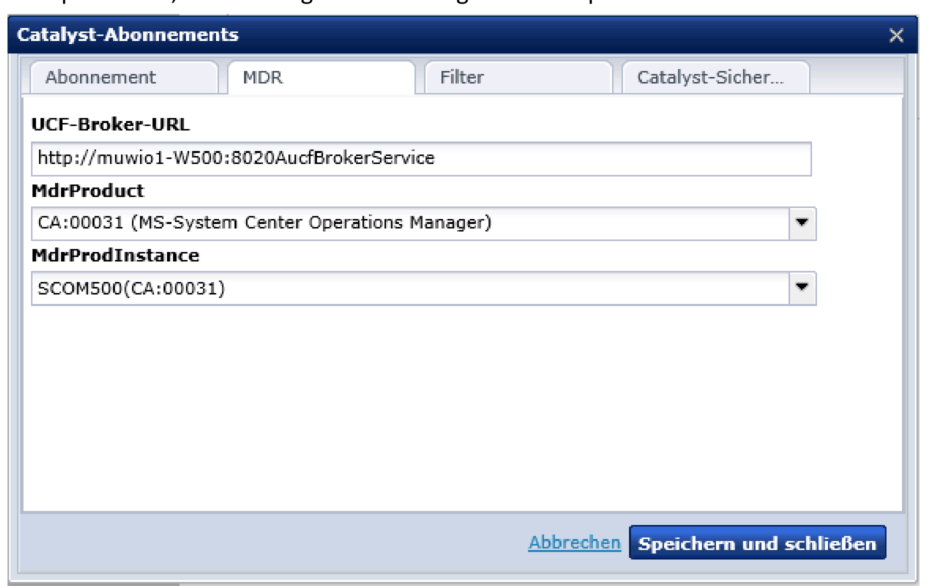
Der Catalyst-Auslöser unterstützt eine Liste von Abonnements, das sich jeweils auf einen Catalyst-Connector mit einem Filter bezieht. Wenn das Produkt ein übereinstimmendes Event vom Catalyst-Connector erhält, wird der angegebene Prozess gestartet.

Sie können die Eigenschaften des Catalyst-Auslösers auf Domänenebene konfigurieren.

Hinweis: Dieser Vorgang zeigt Beispiele für das Festlegen eines Catalyst-Auslösers, um einen Prozess zu starten, wenn Microsoft System Center Operations Manager ein Alarmobjekt erstellt oder aktualisiert. Die Eigenschaften des Alarmobjekts sind als Prozessvariablen verfügbar.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte "Auslöser".
3. Klicken Sie mit der rechten Maustaste auf "Catalyst-Auslöser", und klicken Sie dann auf "Bearbeiten".
4. Klicken Sie im Dialogfeld "Catalyst-Auslöser" auf "Parameter hinzufügen" .
5. Klicken Sie im Fenster "Catalyst-Abonnements" auf die Registerkarte "MDR", und füllen Sie dann die Felder entsprechend aus.
6. Überprüfen Sie, ob Ihre Eingaben dem folgenden Beispiel ähneln:



7. Klicken Sie auf die Registerkarte "Abonnement", und füllen Sie die Felder entsprechend aus.

8. Überprüfen Sie, ob Ihre Eingaben dem folgenden Beispiel ähneln:

Abonnement | MDR | Filter | Catalyst-Sicher...

Abonnementname

SCOMTest

Abonnement-ID

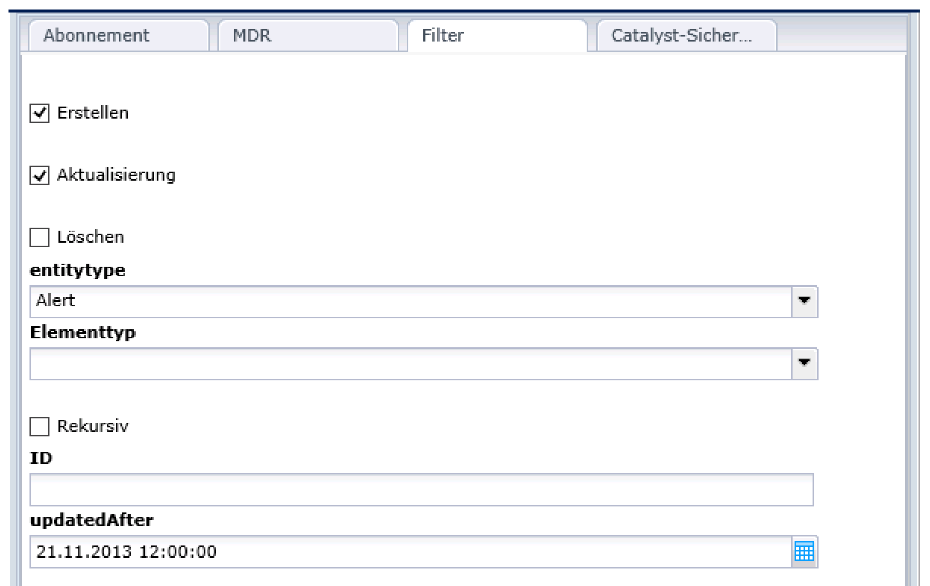
Prozesspfad

Test/TriggerProcess

☑ Aktiviert

9. Klicken Sie auf die Registerkarte "Filter", und füllen Sie die Felder entsprechend aus.

10. Überprüfen Sie, ob Ihre Eingaben dem folgenden Beispiel ähneln:



11. Klicken Sie auf die Registerkarte "Catalyst-Sicherheit".

12. Geben Sie die Anmeldeinformationen in die Felder "Anwendername" und "Kennwort" ein.

13. Klicken Sie für jeden hinzuzufügenden Anspruch unter "Ansprüche" auf die Schaltfläche "Parameter hinzufügen", und füllen Sie dann die Felder "Anspruchsname" und "Anspruchswert" aus.

14. Klicken Sie für jedes hinzuzufügende Kennwort unter "Ansprüche" auf die Schaltfläche "Parameter hinzufügen", und füllen Sie dann die Felder "Anspruchsname" und "Anspruchswert" aus.

15. Klicken Sie auf Speichern und Schließen.

    Das Produkt fügt das Abonnement hinzu, das Sie in der Liste "Abonnement" definiert haben. Um die Definition zu bearbeiten, heben Sie den Eintrag hervor, und klicken Sie dann auf "Bearbeiten".

16. Klicken Sie auf "Speichern".
17. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren der Dateiauslöser-Eigenschaften auf Domänenebene

Mit Domänenadministratorrechten können Sie die Eigenschaften "Dateiauslöser" auf der Domänenebene konfigurieren. Vererbung ist *nicht* der Standard. Um Einstellungen zu verwenden, die Sie auf der Domänenebene konfiguriert haben, konfigurieren Sie "Von Domäne erben" auf der Umgebungsebene, und konfigurieren Sie "Von Umgebung erben" auf der Ebene des Koordinationsrechners.

Wenn Sie "Dateiauslöser" verwenden, um Prozesse zu starten, sucht der Koordinationsrechner im angegebenen Eingabeverzeichnis nach neuen Dateien und verwendet dabei die konfigurierten Intervalle. Das Produkt analysiert den Inhalt jeder Datei, die mit dem angegebenen Namensmuster der Eingabedatei übereinstimmt und löst den angegebenen Prozess aus. Nachdem der Prozess ausgelöst wird, verschiebt das Produkt die Datei in "Verarbeitetes Verzeichnis". Wenn das Produkt den Prozess nicht starten kann, werden die auslösende Datei und eine .err-Datei in das angegebene Fehlerverzeichnis verschoben. Die .err-Datei beschreibt, warum der Auslöser fehlschlägt.

Hinweis: Wenn eine neue Datei und eine vorhandene Datei denselben Namen haben, dann wird die ältere Datei ersetzt.

Bevor Sie die Eigenschaften des Dateiauslösers konfigurieren, erstellen Sie folgende Verzeichnisse:

- Ein Eingabeverzeichnis mit den Schreibberechtigungen, die erforderlich sind, um Auslöserdateien anzunehmen. Um Remote-Auslöser zu ermöglichen, sollten Sie das Verzeichnis zu einem FTP-Ordner zuordnen.
- Ein "Verarbeitetes Verzeichnis", um die erfolgreich verarbeitete Ausgabe zu erhalten.
- Ein Fehlerverzeichnis für die Ausgabe, die nicht verarbeitet werden kann.

Wenn sie nicht vorhanden sind, erstellt das Produkt die Verzeichnisse.

Sie können Dateiauslösereigenschaften auf Domänenebene konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte "Auslöser", klicken Sie mit der rechten Maustaste auf "Dateiauslöser", und klicken Sie auf "Bearbeiten".
3. Füllen Sie im Dialogfeld "Dateiauslöser" die Felder nach Bedarf aus.
4. Stellen Sie sicher, dass Ihre Eingaben gültig sind. Das folgende Beispiel enthält gültige Eingaben.



5. Klicken Sie auf Speichern und Schließen.
6. Klicken Sie auf "Speichern".
7. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren von E-Mail-Auslösereigenschaften auf Domänenebene

Mit Domänenadministratorrechten können Sie die Eigenschaften "E-Mail-Auslöser" auf der Domänenebene konfigurieren. E-Mail-Auslösereigenschaften ermöglichen nur dann das Auslösen von Prozessen, wenn sie übernommen oder auf niedrigeren Ebenen konfiguriert wurden. Um die Vererbung zu erhalten, konfigurieren Sie "Von Domäne erben" auf der Umgebungsebene, und konfigurieren Sie "Von Umgebung erben" auf der Ebene des Koordinationsrechners.

Wenn der E-Mail-Auslöser aktiv ist, wird das E-Mail-Konto (mit Anwendername und Kennwort konfiguriert) nach E-Mails durchsucht. Wenn der E-Mail-Text oder ein Anhang einen gültigen XML-Inhalt enthält, dann verarbeitet das Produkt den Text bzw. den Inhalt. Die Parameter, die das Produkt in der ausgelösten Prozessinstanz erstellt, hängen davon ab, ob die E-Mail einen gültigen XML-Inhalt enthält.

Bevor Sie die Eigenschaften des E-Mail-Auslösers konfigurieren, führen Sie folgende Aufgaben durch:

- Erstellen Sie ein E-Mail-Konto für den Empfang von E-Mails, die Prozesse auslösen.
- Überprüfen Sie, ob der IMAP-Dienst auf dem E-Mail-Server, den Sie als eingehenden E-Mail-Server identifizieren, aktiviert ist.

  Wenn Ihr Unternehmens-E-Mail-Server das Aktivieren des IMAP-Dienstes beschränkt, erstellen Sie einen Proxy-Mail-Server mit aktiviertem IMAP. Geben Sie den Proxy-Server als eingehenden E-Mail-Server an. Konfigurieren Sie dann Ihren Unternehmens-E-Mail-Server, um diesem Proxy-E-Mail-Server die E-Mails weiterzuleiten, die an das konfigurierte Anwenderkonto adressiert sind.
- (Optional) Erstellen Sie einen standardmäßigen Prozess des Domänen-Koordinationsrechners, und speichern Sie ihn im Pfad des standardmäßigen Prozess-Handler. Das Produkt verwendet den Standardprozess nur dann, wenn die E-Mail keinen zulässigen XML-Inhalt enthält. In diesem Fall wird der Standardprozess gestartet, und die folgenden Variablen auf der SMTP-Seite im Prozessdatensatz werden aufgefüllt:

  senderAdd

  Gibt die E-Mail-Adresse des Absenders an.

  senderTime

  Identifiziert die E-Mail-Server-Zeit, zu der die E-Mail gesendet wurde.

  MailBody

  Enthält den vollständigen Inhalt der E-Mail.

  Der Standardprozess bestimmt alle weitere Aktionen.

Sie können die Eigenschaften des E-Mail-Auslösers auf Domänenebene konfigurieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte "Auslöser", klicken Sie mit der rechten Maustaste auf "E-Mail-Auslöser", und klicken Sie dann auf "Bearbeiten".
3. Füllen Sie nach Bedarf die Felder im Dialogfeld "E-Mail-Auslöser" auf der Registerkarte "Allgemeine Eigenschaften" aus.

   Standard-Auslöserprozess (nur Koordinationsrechner)

   Gibt an, wie E-Mails verarbeitet werden sollen, die ungültigen XML-Inhalt im Nachrichtentext oder Anhang enthalten.

   Werte:

   - **Leer**: E-Mails ohne gültigen XML-Auslöserinhalt werden ignoriert.
   - Der vollständige Pfad des Prozesses, den der Domänen-Koordinationsrechner starten soll. (Für jeden Koordinationsrechner kann ein Standardprozess definiert werden.)

   IMAP-Mailserver

   Gibt den Hostnamen oder die IP-Adresse des E-Mail-Servers an, der eingehende E-Mail empfängt. Der Posteingangsordner für das konfigurierte E-Mail-Konto wird nach neuen E-Mails durchsucht. Auf diesem Server muss das IMAP-Protokoll aktiviert sein. Der E-Mail-Auslöser unterstützt kein POP3.

   IMAP-Serverport

   Wenn der Standard-TCP-Port für einen IMAP-Server verwendet wird, geben Sie "143" ein. Wenn ein Nicht-Standard-Port verwendet wird oder sichere Kommunikation auf einem anderen Port eingerichtet wird, erhalten Sie den richtigen einzugebenden Port von einem Administrator.

   Anwendername

   Gibt den Anwendernamen an, der für die Verbindung zum eingehenden E-Mail-Server verwendet werden soll. Beachten Sie die Anforderungen Ihres IMAP-Servers, wenn Sie bestimmen, ob die vollständige E-Mail-Adresse oder der Alias als Anwendername eingegeben werden soll. Der Anwendername "pamadmin@ca.com" ist ein Beispiel für eine vollständige Adresse; "pamadmin" ist der Alias.

   Hinweis: Microsoft Exchange Server akzeptiert sowohl die vollständige E-Mail-Adresse als auch den Alias.

   Kennwort

   Gibt das Kennwort an, das mit dem angegebenen Anwendernamen verbunden ist.

Intervall für E-Mail-Verarbeitung (Sekunden)

Die Frequenz entspricht der Häufigkeit in Sekunden, mit denen CA Process Automation den IMAP-Server nach neuen eingehenden E-Mails im angegebenen Konto durchsucht. Der Anwendername und das Kennwort geben das Konto an.

Standard:

2

E-Mail-Anhänge in Datenbank speichern

Gibt an, ob Anhänge von E-Mails, die CA Process Automation-Prozesse in der Datenbank auslösen, gespeichert werden sollen.

- Aktiviert: CA Process Automation speichert Anhänge von E-Mails in der CA Process Automation-Datenbank und füllt den Datensatz des Prozesses auf, der mit relevanten Information zu den Anhängen gestartet wird.
- Deaktiviert: CA Process Automation speichert keine E-Mail-Anhänge.

SMTP-Postausgangsserver

Gibt den Servernamen für den SMTP-Postausgangsserver an. Wenn eine auslösende E-Mail mit gültigem XML-Inhalt im konfigurierten Konto des IMAP-E-Mail-Servers empfangen wird, wird eine Bestätigungs-E-Mail zurückgeschickt. Die Bestätigungs-E-Mail wird über den SMTP-Postausgangsserver an den Absender zurückgegeben.

SMTP-Serverport

Gibt den Port des Postausgangsservers an.

Standard:

25

Sichere SMTP-Verbindung verwenden

Gibt an, ob der Prozess über eine sichere Verbindung mit dem SMTP-Mailserver ausgeführt werden soll.

- **Ausgewählt**: Der Mail-Server erlaubt eine sichere Verbindung zum SMTP-Mail-Server.
- **Deaktiviert**: Der Mailserver erlaubt keine sichere Verbindung.

Standard:

Gelöscht

4. Klicken Sie auf Speichern und Schließen.
5. Klicken Sie auf "Speichern".
6. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Konfigurieren von SNMP-Auslösereigenschaften auf Domänenebene

Ein Administrator mit Domänenadministratorrechten kann SNMP-Auslösereigenschaften auf Domänenebene konfigurieren. Wenn übernommen, ermöglichen es SNMP-Auslösereigenschaften Prozessen, beim Empfang einer SNMP-Trap ausgelöst zu werden.

Bevor Sie beginnen, SNMP-Auslösereigenschaften zu konfigurieren, überprüfen Sie, ob CA Process Automation auf Port 162 zugreifen kann. Ändern Sie die SNMP-Traps-Listener-Ports in der CA Process Automation-Eigenschaftsdatei, wenn Sie einen alternativen Port verwenden.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration", wählen Sie "Domäne" aus, und klicken Sie auf "Sperren".
2. Klicken Sie auf die Registerkarte "Auslöser", klicken Sie mit der rechten Maustaste auf "SNMP-Auslöser", und klicken Sie dann auf "Bearbeiten".
3. Klicken Sie auf "Parameter hinzufügen".
4. Füllen Sie im Fenster "SNMP-Auslöser" die Felder "Trap-Filter" nach Bedarf aus.

5. Stellen Sie sicher, dass Ihre Eingaben gültig sind.

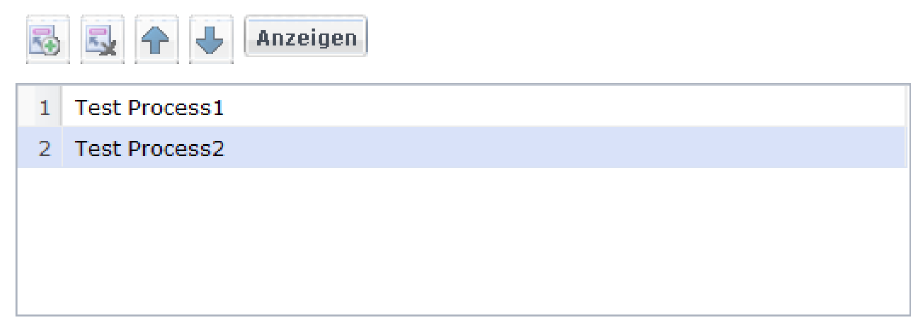
   Folgender Beispielfilter akzeptiert SNMP-Traps von einem beliebigen Host, der folgende Eigenschaften hat:

   - Eine IP-Adresse zwischen "138.42.7.1" und "138.42.7.254" mit einer OID, die mit 1.3.6.1.4.1.[x.x.x.x.x] beginnt
   - Mindestens einen Nutzdatenwert, der mit der Literalzeichenfolgen "Test Payload for trigger" übereinstimmt.

   Wenn das Produkt eine SNMP-Trap mit diesen Kriterien empfängt, wird der Prozess "RunProcess1" im Pfad "/Test" ausgelöst.



6. Klicken Sie nach Bedarf auf die Schaltflächen "Nach oben verschieben" und "Nach unten verschieben", um die Rangfolge der Liste festzulegen. Jeder Filter hat Vorrang vor den Filtern, die nachstehend aufgelistet sind.



7. Klicken Sie auf "Speichern".
8. Wählen Sie "Domäne" aus, und klicken Sie auf "Entsperren".

Weitere Informationen:

Ändern des SNMP-Traps-Listener-Ports (siehe Seite 348)

Ändern des SNMP-Traps-Listener-Ports

Standardmäßig überwacht CA Process Automation Port 162, um SNMP-Traps zu finden, die zum Starten von CA Process Automation-Prozessen entworfen wurden. Wenn Sie Port 162 an Ihrem Standort geschlossen und einen alternativen Port konfiguriert haben, ändern Sie die CA Process Automation-Konfiguration für diesen Port in der Datei "OasisConfig.properties". Starten Sie dann den Koordinationsrechner-Service neu.

Sie können den Port ändern, auf dem CA Process Automation nach SNMP-Traps sucht.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei dem Server an, auf dem der Domänen-Koordinationsrechner konfiguriert ist.
2. Navigieren Sie zum folgenden Ordner oder Verzeichnis:

   `*Installationsverzeichnis*/server/c2o/.config/`
3. Öffnen Sie die Datei "OasisConfig.properties".
4. Ändern Sie den Wert in der folgenden Zeile von "162" in die Portnummer, die Sie für SNMP-Traps verwenden.

   `oasis.snmptrigger.service.port=162`
5. Speichern Sie die Datei.
6. Starten Sie den Koordinationsrechner-Service neu.
   a. Stoppen Sie den Koordinationsrechner (siehe Seite 206).
   b. Starten Sie den Koordinationsrechner (siehe Seite 207).

   Sobald der Service neu startet, beginnt CA Process Automation damit, den von Ihnen konfigurierten Port abzuhören. CA Process Automation sucht nach neuen SNMP-Traps, die den konfigurierten Kriterien im SNMP-Auslöser entsprechen.

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Kapitel 14: Anwenderressourcen verwalten

Sie können Ressourcen für Anwender, Koordinationsrechner, und Agenten über das Auswahlmenü "Anwenderressourcen verwalten" der Registerkarte "Konfiguration" verwalten.

Das Auswahlmenü "Anwenderressourcen verwalten" enthält drei Ordner unter "Repository":

- Agentenressourcen
- Koordinationsrechnerressourcen
- Anwenderressourcen, der den Unterordner "VBS_Resources" enthält.

  Hinweis: Sie können Unterordner nur unter dem Ordner "Anwenderressource" hinzufügen.

Anwender, denen die Berechtigung "Configuration_User_Resources" in der Richtlinie des Konfigurationsbrowsers in CA EEM erteilt wurde, können Ressourcen unter dem Ordner "Anwenderressourcen" verwalten. Allerdings können nur Anwender, denen die Berechtigung "Domain_Administrator" der Domänenrichtlinie gewährt wurde, auf Ordner der Koordinationsrechnerressourcen und Agentenressourcen zugreifen. Mitglieder der Standardgruppe "PAMAdmins" haben beide Berechtigungen.

Dieses Kapitel enthält folgende Themen:

Informationen über die Verwaltung der Anwenderressourcen

Ressourcenmanagement erfordert bestimmte Berechtigungen für verschiedene Aktivitäten. Anwender, die zur standardmäßigen PAMAdmins-Gruppe gehören (die Gruppe mit vollen Berechtigungen), können jede Aktivität des Ressourcenmanagements ausführen.

Anwender in anwenderspezifischen Gruppen, die anwenderspezifische Richtlinien haben, müssen grundlegenden Zugriff und eine oder beide der folgenden Berechtigungen haben:

PAM40-Umgebungsrichtlinie: Environment_Configuration_Admin (Konfigurationsadministrator)

Anwender mit Berechtigungen "Environment_Configuration_Admin" (Konfigurationsadministrator) können jede Art von Datei in Anwenderressourcen hochladen, ändern oder löschen. Zum Beispiel:

- Eine JAR-Datei für die Verwendung mit dem Operator "Java aufrufen".
- Ein Skript für die Verwendung mit dem Operator "Skript ausführen".
- Ein Bild.

PAM40-Domänenrichtlinie: Domain_Admin (Administrator)

Anwender mit Berechtigungen "Domain_Admin" (Administrator) können folgende Aufgaben ausführen:

- Hinzufügen von Ressourcen in den Ordner "Koordinationsrechnerressourcen" oder in den Ordner "Agentenressourcen"
- Bearbeiten des Inhalts einer Ressource und das erneute Hinzufügen der Ressource; Aktualisieren der beschreibenden Felder
- Löschen einer zuvor hochgeladenen Koordinationsrechnerressource oder Agentenressource

Hinweis: Die Vorgänge für das Bearbeiten und Löschen von Koordinationsrechnerressourcen und Agentenressourcen ähneln den Vorgängen für das Bearbeiten und Löschen von Anwenderressourcen.

Unterschiede zwischen Anwenderressourcen und Agenten- oder Koordinationsrechnerressourcen sind Folgende:

Anwenderressourcen

- Nach einem Neustart schließt der "classpath" des Agenten oder Koordinationsrechners keine Ressourcen ein, die auf Anwenderressourcen hochgeladen wurden.
- Sie können Unterordner innerhalb des Ordners "Anwenderressourcen" erstellen.
- Sie benötigen keine Domain_Admin-Rechte (Administrator).

Agentenressourcen und Koordinationsrechnerressourcen

- Nach einem Neustart schließt der "classpath" des Agenten oder Koordinationsrechners Ressourcen ein, die auf Agentenressourcen und Koordinationsrechnerressourcen hochgeladen wurden.
- Sie können keine Unterordner innerhalb der Ordner "Agentenressourcen" und "Koordinationsrechnerressourcen" erstellen.
- Sie benötigen die Rechte "Domain_Admin" (Administrator).

So stellen Sie JDBC-Treiber für Datenbankoperatoren bereit

Sie können JBDC-Treiber für Datenbankoperatoren entweder während oder nach der Installation von CA Process Automation installieren. Nur Prozesse mit Datenbankoperatoren benötigen einen JBDC-Treiber.

Während der Installation werden die JDBC-Treiber, die bei der Installation der Drittanbieter-Software hochgeladen wurden, angezeigt aber nicht ausgewählt. Sie können die JDBC-Treiber für MySQL, Microsoft SQL Server und Oracle auswählen. Sie können auch andere JAR-Dateien hinzufügen, die Sie in ein lokales Verzeichnis kopiert haben.

Nach der Installation können Sie JAR-Dateien hochladen, die JDBC-Treiber für Datenbankoperatoren enthalten, indem Sie das Auswahlmenü "Anwenderressourcen verwalten" auf der Registerkarte "Konfiguration" verwenden. CA Process Automation stellt die hochgeladenen JAR-Dateien entweder für Koordinationsrechner oder für Agenten bereit, je nachdem, welchen Ordner Sie beim Hochladen auswählen. Weitere Informationen finden Sie in den entsprechenden Themen:

- Hochladen von Koordinationsrechnerressourcen (siehe Seite 352).
- Hochladen von Agentenressourcen (siehe Seite 354).

Hochladen von Koordinationsrechnerressourcen

Nach der Installation zeigt der Ordner "Koordinationsrechnerressourcen" nur die JDBC JAR-Dateien an, die während der Installation hinzugefügt wurden. Nachdem Sie das Auswahlmenü "Anwenderressourcen verwalten" verwendet haben, um den Ordner "Koordinationsrechnerressourcen" zu aktualisieren, zeigt der Ordner "Koordinationsrechnerressourcen" auch die hochgeladenen JAR-Dateien an.

Sie können eine JAR-Datei zum Ordner "Koordinationsrechnerressourcen" auf dem Domänen-Koordinationsrechner hochladen. Wenn Sie den Domänen-Koordinationsrechner neu starten, stellt CA Process Automation die Datei für den Domänen-Koordinationsrechner bereit. Der Domänen-Koordinationsrechner spiegelt (kopiert) die Datei an dem konfigurierten Spiegelungsintervall wider, nach dem Sie die anderen Koordinationsrechner neu starten. Wenn die Koordinationsrechner neu starten, wird die gespiegelte Datei zur Verwendung verfügbar.

Hinweis: Die Spiegelung bezieht sich auf alle Koordinationsrechner in der Domäne. Für geclusterte Koordinationsrechner bezieht sich die Spiegelung in jedem Cluster auf alle Knoten.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie auf das Auswahlmenü Anwenderressourcen verwalten, und erweitern Sie den Ordner Repository.
3. Wählen Sie den Ordner Koordinationsrechnerressourcen aus.
4. Klicken Sie auf Neu.

   Der Bereich Neue Ressource hinzufügen: "Unbenannt" wird geöffnet.
5. Geben Sie die Hochladedetails entsprechend in den folgenden Feldern an:
   a. Geben Sie den Namen der Ressource im Feld Ressourcenname ein.

      Folgendes Beispiel ist sinnvoll, um den Ressourcennamen anzugeben, wenn Sie einen JDBC-Treiber hochladen:

      `Datenbankname-Treiber`

      Datenbankname

         Definiert den Namen des RDBMS. Zum Beispiel: Oracle-Treiber, MySQL-Treiber oder Sybase-Treiber.
   b. Klicken Sie auf "Durchsuchen", navigieren Sie zu dem Speicherort, in dem Sie die JAR-Datei gespeichert haben, und wählen Sie die Zieldatei aus. Dadurch wird das Feld Ressourcendatei aufgefüllt.

c. Wählen Sie aus der Drop-down-Liste Modulname einen anwenderspezifischen Modulnamen aus.

d. (Optional) Geben Sie eine Beschreibung der Ressource in das Feld Beschreibung ein.

6. Überprüfen Sie Ihre Eingabe, und klicken Sie auf "Speichern".

   Eine Zeile mit Ihrer Eingabe wird angezeigt.

☑	Name	Dateityp	Dateipfad	Modul
☑	Sybase Driver	jar	.c2oserverresources/lib/jconn2.jar	Sybase Driver

   CA Process Automation kopiert die hochgeladene Ressource zu den folgenden Pfaden:

   `*Installationsverzeichnis*/Server/c2o/ext-lib`

   `*Installationsverzeichnis*/Server/c2o/.c2orepository/.c2oserverresources/lib`

   Installationsverzeichnis

   Definiert das Verzeichnis auf dem Server, in dem der Domänen-Koordinationsrechner installiert wurde.

7. Starten Sie den Domänen-Koordinationsrechner erneut. Das heißt, halten Sie den Koordinationsrechner an, (siehe Seite 206) und starten Sie dann den Koordinationsrechner (siehe Seite 207).

   Wenn der Domänen-Koordinationsrechner neu startet, stellt das System alle hochgeladenen JAR-Dateien für die Domänen-Koordinationsrechnerressourcen bereit. Das bedeutet, dass CA Process Automation die JAR-Dateien in den "classpath" des Domänen-Koordinationsrechners stellt.

8. Starten Sie nach der Spiegelung alle anderen Koordinationsrechner neu.

   Das System stellt alle hochgeladenen JAR-Dateien auf allen Koordinationsrechnern bereit. Das heißt, das System stellt die JAR-Dateien in die "classpaths" der Koordinationsrechner.

   Hinweis: Starten Sie für geclusterte Koordinationsrechner jeden Knoten neu.

Hochladen von Agentenressourcen

Anwender mit der Berechtigung "Domänenadministrator" können Ressourcen in den Ordner "Agentenressourcen" auf dem Domänen-Koordinationsrechner hochladen. Die hochgeladene Ressource kann eine JAR-Datei sein, zum Beispiel ein JDBC-Treiber. Die hochgeladenen Agentenressourcen werden im konfigurierten Spiegelungsintervall gespiegelt. Starten Sie nach der Spiegelung die Agenten neu. Neu gestartete Agenten können die hochgeladenen Agentenressourcen verwenden.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA Process Automation, und melden Sie sich an (siehe Seite 18).
2. Klicken Sie auf die Registerkarte Konfiguration.
3. Klicken Sie auf das Auswahlmenü Anwenderressourcen verwalten, und erweitern Sie den Ordner Repository.
4. Wählen Sie den Ordner Agentenressourcen aus, und klicken Sie auf Neu.

   Das Feld Neue Ressource hinzufügen: "Unbenannt" wird angezeigt.

5. Stellen Sie Details für das Hochladen bereit, indem Sie bei Bedarf folgende Feldbeschreibungen verwenden.
   a. Geben Sie den Namen der Ressource im Feld Ressourcenname ein.

      Wenn Sie einen JDBC-Treiber hochladen, geben Sie *Datenbankname*-Treiber ein, wobei *Datenbankname* das RDBMS ist. Zum Beispiel: Oracle-Treiber, MySQL-Treiber oder Sybase-Treiber.

   b. Klicken Sie auf "Durchsuchen", navigieren Sie zu dem Speicherort, in dem Sie die JAR-Datei gespeichert haben, und wählen Sie die Zieldatei aus.

      Dadurch wird das Feld Ressourcendatei mit der Datei und ihrem Pfad aufgefüllt.

   c. (Optional) Wählen Sie einen anwenderspezifischen Modulnamen aus der Drop-down-Liste Modulname aus.
   d. (Optional) Geben Sie im Feld Ressourcenbeschreibung eine aussagekräftige Beschreibung ein.

6. Überprüfen Sie Ihre Eingabe. Klicken Sie anschließend auf Speichern.

   Eine Zeile mit Ihrer Eingabe wird angezeigt.

   CA Process Automation kopiert die hochgeladenen Ressourcen, z. B. einen JDBC-Treiber, in den folgenden Pfad, bei dem *Installationsverzeichnis* das Verzeichnis auf dem Server ist, auf dem der Domänen-Koordinationsrechner installiert wurde.

   Installationsverzeichnis/server/c2o/.c2orepository/.c2oagentresources/lib/drivers/jars

7. Nachdem die Spiegelung abgeschlossen ist, starten Sie die Agenten neu, bei denen Sie die hochgeladenen JAR-Dateien benötigen. Die JAR-Dateien werden in den "classpath" der neu gestarteten Agenten gestellt.

   Hinweis: Weitere Informationen zum Neustart von Agenten finden Sie unter So starten Sie einen Agenten oder halten ihn an.

Hochladen von Anwenderressourcen

Hochladen bedeutet, einen Ordner unter dem Ordner "Anwenderressource" zu erstellen und zur Ressource zu navigieren, die hochgeladen werden soll. CA Process Automation fügt die Ressource zu der Baumstruktur "Anwenderressource" hinzu und lädt die Ressource hoch.

Sehen Sie sich die folgenden Vorgänge an:

- Hinzufügen einer Ressource zu Anwenderressourcen (siehe Seite 356).
- Löschen einer Ressource aus den Anwenderressourcen (siehe Seite 357).
- Ändern einer Ressource in den Anwenderressourcen (siehe Seite 358).

Hinweis: Um den Ressourcenpfad zu ändern, löschen Sie die Ressource, und fügen Sie sie unter einem anderen Pfad erneut hinzu.

Ressource für die Ausführung des Operators "Java aufrufen" - Beispiel

Der Installationsprozess fügt dem Ordner "Anwenderressource" eine Ressource unter "Repository" im Auswahlmenü "Anwenderressourcen verwalten" auf der Registerkarte "Konfiguration" hinzu. Die JAR-Datei "MyAccount.jar" befindet sich im Ordner "Invoke_Java_Op_Example_jars". Sie können die Datei "MyAccount.jar" verwenden, um das Java-Beispiel auszuführen, das im Feld "Erforderliche Hauptmethode" des Operators "Java aufrufen" angegeben ist.



Hinzufügen einer Ressource zu Anwenderressourcen

Anwender mit administrativen Berechtigungen können Skripts zum Ordner "Anwenderressourcen" in der globalen Repository hinzufügen. Das Produkt spiegelt hochgeladene Anwenderressourcen im konfigurierten Intervall zu anderen Koordinationsrechnern und Agenten in der Domäne. Koordinationsrechner und Agenten können auf Anwenderressourcen nach Referenz zugreifen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Klicken Sie auf das Auswahlmenü "Anwenderressourcen verwalten".
3. Erweitern Sie den Ordner "Repository" und den Ordner "Anwenderressourcen".
4. Wählen Sie den Ordner "Anwenderressourcen" oder einen Unterordner aus, und klicken Sie auf "Neu".

5. Füllen Sie die Felder im Bereich "Neue Ressource hinzufügen" nach Bedarf aus.
6. Überprüfen Sie Ihre Eingaben, und klicken Sie dann auf "Speichern".

   Die Liste im Bereich "Anwenderressourcen" zeigt den Namen, den Typ, den Pfad, das Modul und die Beschreibung der hochgeladenen Datei an.

Das Produkt kopiert die hochgeladenen Anwenderressourcen in den folgenden Pfad:

install_dir/server/c2o/.c2orepository/.c2ouserresources/...

Installationsverzeichnis

Definiert das Verzeichnis auf dem Server, in dem der Domänen-Koordinationsrechner installiert wurde.

Das Produkt erstellt nach Bedarf Unterordner, um den Pfad aus dem Ordner "Anwenderressourcen" zur Ressource zu verwalten.

Weitere Informationen:

Laden von Catalyst-Deskriptoren (siehe Seite 292)

Löschen einer Ressource aus den Anwenderressourcen

Sie können eine Ressource löschen, wie z. B. ein Skript oder eine JAR-Datei, das bzw. die Sie dem Ordner "Anwenderressource" hinzugefügt haben.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Klicken Sie auf das Auswahlmenü "Anwenderressourcen verwalten".
3. Erweitern Sie den Ordner "Repository". Erweitern Sie den Ordner "Anwenderressource".
4. Klicken Sie auf den Ordner, in dem sich die Ressource befindet.
5. Klicken Sie auf die Zeile mit dem Namen der zu löschenden Ressource, und klicken Sie dann auf "Löschen".

Hinweis: Wenn Sie die letzte Ressource aus einem Unterordner von "Anwenderressource" löschen, dann wird auch dieser Unterordner gelöscht.

Ändern einer Ressource in den Anwenderressourcen

Sie können eine Ressource folgendermaßen ändern:

- Sie können Text in jedem beliebigen angezeigten Feld ändern, außer dem Ressourcenpfad. Diese Aktion ist möglich, egal ob Sie "Datei ersetzen" auswählen oder nicht.
- Sie können eine bearbeitete Ressource hochladen, (wie z. B. ein Skript oder eine JAR-Datei), die Sie zuvor zu den Anwenderressourcen hinzugefügt haben. Diese Aktion ist nur möglich, wenn Sie "Datei ersetzen" auswählen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Konfiguration".
2. Klicken Sie auf das Auswahlmenü "Anwenderressourcen verwalten".
3. Erweitern Sie den Ordner "Repository" und den Ordner "Anwenderressourcen".
4. Klicken Sie auf den Ordner, in dem sich die Ressource befindet.
5. Klicken Sie mit der rechten Maustaste auf die Zeile, die den Namen der zu ändernden Ressource anzeigt, und wählen Sie "Bearbeiten" aus.

   Die Seite "Ressource" wird geöffnet.
6. (Optional) Ändern Sie die Ressourceninformationen. Sie können folgende Felder bearbeiten:
   - Ressourcenname
   - Modulname
   - Ressourcenbeschreibung
7. Legen Sie das Kontrollkästchen "Datei ersetzen" folgendermaßen fest:
   - Wenn Ihre *einzigen* Änderungen an der Ressource aktualisierte Felder auf der Seite "Ressourcen" sind, deaktivieren Sie das Kontrollkästchen "Datei ersetzen" und klicken Sie auf "Speichern".
   - Wenn Sie Ihre lokale Kopie der Ressourcendatei aktualisiert haben und Ihre Aktualisierungen hochladen wollen:
     a. Wählen Sie "Datei ersetzen" aus.
     b. Klicken Sie auf "Durchsuchen".
     c. Navigieren Sie zur aktualisierten Datei und klicken Sie auf "Öffnen".
     d. Klicken Sie auf "Speichern".

   Der Ordner "Anwenderressourcen" enthält nun die aktualisierte Datei. Die Seite "Ressourcen" enthält Text für alle Felder, die Sie geändert haben.

Kapitel 15: Audit-Anwenderaktionen

CA Process Automation stellt für Konfigurationsobjekte (Domäne, Umgebungen, Agenten und Koordinationsrechner) und Bibliotheksobjekte Audit-Pfade bereit, um Aktivitäten zu verfolgen und aufzuzeichnen (Ordner und Automatisierungsobjekte). Ein Domänenadministrator kann den Audit-Pfad für die Domäne anzeigen. Ein Konfigurationsadministrator für die Umgebung kann den Audit-Pfad für eine Umgebung anzeigen. Ein Endanwender mit Anwenderberechtigung für eine Umgebung kann den Audit-Pfad für ein Objekt anzeigen.

Dieses Kapitel enthält folgende Themen:

Anzeigen des Audit-Pfads für die Domäne

Administratoren können den Audit-Pfad der Domäne anzeigen.

Der Audit-Pfad der Domäne überwacht folgende Aktionen:

- Domäne ist gesperrt oder entsperrt.
- Domäneneigenschaft wird geändert.
- Domänen-Koordinationsrechner wird geändert.
- Umgebung wird erstellt, gelöscht, gesperrt, entsperrt oder umbenannt.
- Koordinationsrechner wird hinzugefügt, gelöscht oder umbenannt.
- Agent wird hinzugefügt, gelöscht oder umbenannt.
- Agentenreferenz wurde Kontaktpunkt "Kontaktpunktname" zugewiesen.

Folgendes Beispiel zeigt den Audit-Pfad für das Zuweisen eines Kontaktpunkts zu einem Agenten. Zwei der Spalten werden ausgeblendet.



Gehen Sie folgendermaßen vor:

1. Wählen Sie die Registerkarte "Konfiguration" aus.
2. Wählen Sie im Auswahlmenü "Konfigurationsbrowser" den Knoten "Domäne" aus.
3. Klicken Sie im Bereich "Inhalt" auf die Registerkarte "Audit-Pfade".

   Die Registerkarte "Audit-Pfade" zeigt folgende Informationen für alle Datensätze an:

   - Objektname
   - Letzte Aktualisierung:
   - Anwendername
   - Aktionstyp
   - Beschreibung

4. (Optional) Um die Audit-Pfade in einer bestimmten Spalte zu sortieren, wählen Sie "Aufsteigend sortieren" oder "Absteigend sortieren" aus der Drop-down-Liste der Zielspalte aus.

   Um zum Beispiel einen bestimmten Anwender zu überwachen, aktivieren Sie eine Sortierungsoption in der Drop-down-Liste der Spalte "Anwendername", und scrollen Sie dann zum entsprechenden Datensatz.

5. (Optional) Um die Anzahl der Datensätze zu ändern, die das Produkt auf einer Seite anzeigt, wählen Sie einen Wert aus der Drop-down-Liste "Zeilen pro Seite" aus.
6. Prüfen Sie die Datensätze im Audit-Pfad.

   Wenn die Audit-Datensätze mehrere Seiten umfassen, verwenden Sie die Navigationsschaltflächen der Symbolleiste, um die erste Seite, die vorherige Seite, die nächste Seite oder die letzte Seite anzuzeigen.

Anzeigen des Audit-Pfads für eine Umgebung

Mit Zugriffsrechten der Konfigurationsadministratoren können Sie den Audit-Pfad der Umgebung anzeigen.

Der Audit-Pfad der Umgebung überwacht folgende Aktionen:

- Die Umgebung ist gesperrt oder nicht gesperrt. Die Eigenschaft der Umgebung wird geändert.
- Umgebung wird erstellt oder gelöscht.
- Umgebung oder Objekt in der Umgebung wird umbenannt.
- Kontaktpunkt wird hinzugefügt, gelöscht oder umbenannt.
- Kontaktpunktgruppe wird hinzugefügt oder gelöscht.
- Hostgruppe wird hinzugefügt oder gelöscht.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie im Auswahlmenü "Konfigurationsbrowser" den Knoten "Domäne" ein, und wählen Sie die zu überwachende Umgebung aus (zum Beispiel die Standardumgebung).
3. Klicken Sie im Bereich "Inhalt" auf die Registerkarte "Audit-Pfade".

   Die Registerkarte "Audit-Pfade" zeigt folgende Informationen für alle Datensätze an:

   - Objektname
   - Letzte Aktualisierung:
   - Anwendername
   - Aktionstyp
   - Beschreibung
4. (Optional) Um die Audit-Pfade in einer bestimmten Spalte zu sortieren, wählen Sie "Aufsteigend sortieren" oder "Absteigend sortieren" aus der Drop-down-Liste der Zielspalte aus.

   Um zum Beispiel einen bestimmten Anwender zu überwachen, aktivieren Sie eine Sortierungsoption in der Drop-down-Liste der Spalte "Anwendername", und scrollen Sie dann zum entsprechenden Datensatz.
5. (Optional) Um die Anzahl der Datensätze zu ändern, die das Produkt auf einer Seite anzeigt, wählen Sie einen Wert aus der Drop-down-Liste "Zeilen pro Seite" aus.
6. Prüfen Sie die Datensätze im Audit-Pfad.

   Wenn die Audit-Datensätze mehrere Seiten umfassen, verwenden Sie die Navigationsschaltflächen der Symbolleiste, um die erste Seite, die vorherige Seite, die nächste Seite oder die letzte Seite anzuzeigen.

Anzeigen des Audit-Pfads für einen Koordinationsrechner

Mit Leseberechtigungen für ein Konfigurationsobjekt können Sie den zugeordneten Audit-Pfad anzeigen. Zum Anzeigen des Audit-Pfades für Konfigurationsobjekte sind Zugriffsrechte erforderlich, die "Umgebungsanwender" und "Konfigurationsbrowser öffnen" enthalten.

Der Audit-Pfad des Koordinationsrechners überwacht folgende Aktionen:

- Koordinationsrechner ist gesperrt oder entsperrt.
- Koordinationsrechnereigenschaft wird geändert.
- Koordinationsrechner wurde in Quarantäne gestellt oder nicht in Quarantäne gestellt.
- Koordinationsrechner ist einem Kontaktpunkt zugeordnet oder die Zuordnung von einem Kontaktpunkt wurde entfernt.
- Koordinationsrechner ist umbenannt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie im Auswahlmenü "Konfigurationsbrowser" den Knoten "Koordinationsrechner" ein, und wählen Sie den Ziel-Koordinationsrechner aus.
3. Klicken Sie im Bereich "Inhalt" auf die Registerkarte "Audit-Pfade".

   Die Registerkarte "Audit-Pfade" zeigt folgende Informationen für alle Datensätze an:

   - Objektname
   - Letzte Aktualisierung:
   - Anwendername
   - Aktionstyp
   - Beschreibung
4. (Optional) Um die Audit-Pfade in einer bestimmten Spalte zu sortieren, wählen Sie "Aufsteigend sortieren" oder "Absteigend sortieren" aus der Drop-down-Liste der Zielspalte aus.

   Um zum Beispiel einen bestimmten Anwender zu überwachen, aktivieren Sie eine Sortierungsoption in der Drop-down-Liste der Spalte "Anwendername", und scrollen Sie dann zum entsprechenden Datensatz.

5. (Optional) Um die Anzahl der Datensätze zu ändern, die das Produkt auf einer Seite anzeigt, wählen Sie einen Wert aus der Drop-down-Liste "Zeilen pro Seite" aus.
6. Prüfen Sie die Datensätze im Audit-Pfad.

   Wenn die Audit-Datensätze mehrere Seiten umfassen, verwenden Sie die Navigationsschaltflächen der Symbolleiste, um die erste Seite, die vorherige Seite, die nächste Seite oder die letzte Seite anzuzeigen.

Anzeigen des Audit-Pfads für einen Agenten

Mit Leseberechtigungen für ein Konfigurationsobjekt können Sie den zugeordneten Audit-Pfad anzeigen. Zum Anzeigen des Audit-Pfades für Konfigurationsobjekte sind CA EEM-Zugriffsrechte erforderlich, die "Umgebungsanwender" und "Konfigurationsbrowser öffnen" enthalten.

Der Audit-Pfad des Agenten überwacht folgende Aktionen:

- Eine Operatorkategorie ist auf der Registerkarte "Module" aktiviert, und ein konfigurierter Wert wird geändert.
- Der Agent wurde in Quarantäne gestellt oder nicht in Quarantäne gestellt.
- Der Agent ist gesperrt oder entsperrt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Blenden Sie im Auswahlmenü "Konfigurationsbrowser" den Knoten "Agenten" ein, und wählen Sie den Zielagenten aus.
3. Klicken Sie im Bereich "Inhalt" auf die Registerkarte "Audit-Pfade".

   Die Registerkarte "Audit-Pfade" zeigt folgende Informationen für alle Datensätze an:

   - Objektname
   - Letzte Aktualisierung:
   - Anwendername
   - Aktionstyp
   - Beschreibung
4. (Optional) Um die Audit-Pfade in einer bestimmten Spalte zu sortieren, wählen Sie "Aufsteigend sortieren" oder "Absteigend sortieren" aus der Drop-down-Liste der Zielspalte aus.

   Um zum Beispiel einen bestimmten Anwender zu überwachen, aktivieren Sie eine Sortierungsoption in der Drop-down-Liste der Spalte "Anwendername", und scrollen Sie dann zum entsprechenden Datensatz.

5. (Optional) Um die Anzahl der Datensätze zu ändern, die das Produkt auf einer Seite anzeigt, wählen Sie einen Wert aus der Drop-down-Liste "Zeilen pro Seite" aus.

6. Prüfen Sie die Datensätze im Audit-Pfad.

   Wenn die Audit-Datensätze mehrere Seiten umfassen, verwenden Sie die Navigationsschaltflächen der Symbolleiste, um die erste Seite, die vorherige Seite, die nächste Seite oder die letzte Seite anzuzeigen.

Anzeigen des Audit-Pfads für einen Kontaktpunkt, eine Kontaktpunktgruppe oder eine Hostgruppe

Mit Leseberechtigungen für ein Konfigurationsobjekt können Sie den zugeordneten Audit-Pfad anzeigen. Zum Anzeigen des Audit-Pfades für Konfigurationsobjekte sind Zugriffsrechte erforderlich, die "Umgebungsanwender" und "Konfigurationsbrowser öffnen" enthalten.

Die Audit-Pfade "Kontaktpunkt", "Kontaktpunktgruppe" und "Hostgruppe" überwachen folgende Aktionen:

- Der Kontaktpunkt ist erstellt
- Der Agent wurde dem Kontaktpunkt zugewiesen
- Die Kontaktpunktgruppe ist erstellt
- Die Kontaktpunkt wird einer Gruppe hinzugefügt
- Die Kontaktpunktgruppe ist umbenannt
- Die Hostgruppe ist erstellt

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Konfiguration.
2. Erweitern Sie im Auswahlmenü "Konfigurationsbrowser" den Knoten "Domäne". Blenden Sie dann den Knoten "Umgebung" ein, der den Zielkontaktpunkt, die Kontaktpunktgruppe oder die Hostgruppe enthält.
3. Blenden Sie den entsprechenden Knoten ein (Alle Kontaktpunkte, Alle Kontaktpunktgruppen oder Alle Hostgruppen), und wählen Sie den Zielkontaktpunkt, die Kontaktpunktgruppe oder die Hostgruppe aus.

4. Klicken Sie im Bereich "Inhalt" auf die Registerkarte "Audit-Pfade".

   Die Registerkarte "Audit-Pfade" zeigt folgende Informationen für alle Datensätze an:

   - Objektname
   - Letzte Aktualisierung:
   - Anwendername
   - Aktionstyp
   - Beschreibung

5. (Optional) Um die Audit-Pfade in einer bestimmten Spalte zu sortieren, wählen Sie "Aufsteigend sortieren" oder "Absteigend sortieren" aus der Drop-down-Liste der Zielspalte aus.

   Um zum Beispiel einen bestimmten Anwender zu überwachen, aktivieren Sie eine Sortierungsoption in der Drop-down-Liste der Spalte "Anwendername", und scrollen Sie dann zum entsprechenden Datensatz.

6. (Optional) Um die Anzahl der Datensätze zu ändern, die das Produkt auf einer Seite anzeigt, wählen Sie einen Wert aus der Drop-down-Liste "Zeilen pro Seite" aus.

7. Prüfen Sie die Datensätze im Audit-Pfad.

   Wenn die Audit-Datensätze mehrere Seiten umfassen, verwenden Sie die Navigationsschaltflächen der Symbolleiste, um die erste Seite, die vorherige Seite, die nächste Seite oder die letzte Seite anzuzeigen.

Anzeigen des Audit-Pfads für einen Bibliotheksordner

Administratoren können den Audit-Pfad für einen ausgewählten Ordner in der Bibliothek anzeigen. Das Produkt schreibt folgende Aktionen für Ordner in einer Bibliothek in die Protokolle:

- Erstellt
- Umbenannt
- Gelöscht
- Erstellen oder löschen von Automatisierungsobjekten
- Abrufen von Automatisierungsobjekten oder Ordnern aus dem Papierkorb
- Ändern von Berechtigungen für Ordner einschließlich Links zu alten und neuen ACLs

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Bibliothek, und wählen Sie einen Koordinationsrechner aus der Drop-down-Liste Koordinationsrechner aus.
2. Navigieren Sie zu dem Ordner, der den zu überwachenden Ordner enthält.
3. Klicken Sie im Bereich "Inhalt" mit der rechten Maustaste auf den zu überwachenden Ordner, und wählen Sie "Eigenschaften" aus.
4. Klicken Sie im Bereich "Eigenschaften" auf die Registerkarte "Audit-Pfade".

   Die Registerkarte "Audit-Pfade" zeigt folgende Informationen für alle Datensätze an:

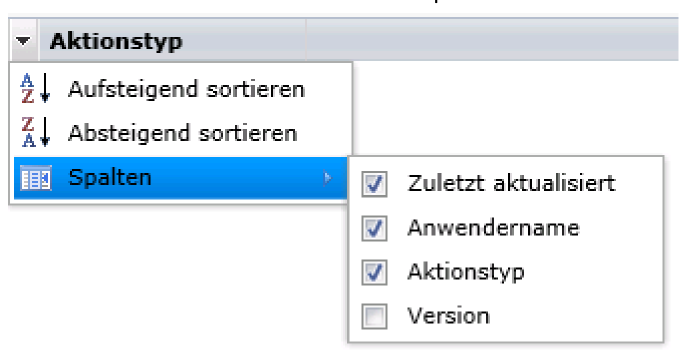
   - Letzte Aktualisierung:
   - Anwendername
   - Aktionstyp
5. (Optional) Um die Audit-Pfade in einer bestimmten Spalte zu sortieren, wählen Sie "Aufsteigend sortieren" oder "Absteigend sortieren" aus der Drop-down-Liste der Zielspalte aus.

6. (Optional) Geben Sie an, welche Spalten das Produkt anzeigt:

   a. Wählen Sie "Spalten" aus der Drop-down-Liste aus einer beliebigen Spaltenüberschrift aus.

   b. Deaktivieren Sie (Ausblenden) oder aktivieren Sie (Einblenden) nach Bedarf die Kontrollkästchen der Spalten.

   Um zum Beispiel die Spalte "Version" anzuzeigen, aktivieren Sie das Kontrollkästchen "Version" im Menü "Spalten".



7. Prüfen Sie die Datensätze im Audit-Pfad.

Anzeigen des Audit-Pfads für ein offenes Automatisierungsobjekt

Administratoren können den Audit-Pfad für ein offenes Automatisierungsobjekt anzeigen. Das Produkt schreibt folgende Aktionen für Automatisierungsobjekte in die Protokolle:

- Erstellen
- Löschen
- Einchecken und Auschecken
- Umbenennen
- Exportieren und Importieren
- Ändern von Berechtigungen für Automatisierungsobjekte einschließlich Links zu alten und neuen ACLs
- Abrufen von Automatisierungsobjekten aus dem Papierkorb
- Ändern der festgelegten aktuellen Version
- Erstellen oder Aktualisieren der Release-Version
- Hinzufügen einer Release-Versions-Eigenschaft
- Aktualisieren eines Automatisierungsobjekts (z. B. eines Ablaufplans) ohne Auschecken
- Verfügbar oder nicht verfügbar Machen von anwenderspezifischen Operatorobjekten
- Aktivieren oder Deaktivieren von Ablaufplänen

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Bibliothek, und wählen Sie einen Koordinationsrechner aus der Drop-down-Liste Koordinationsrechner aus.
2. Navigieren Sie zu dem Ordner, der die zu überwachende Automatisierungsobjektinstanz enthält.
3. Klicken Sie im Bereich "Inhalt" mit der rechten Maustaste auf die Automatisierungsobjektinstanz des Ziels, und wählen Sie "Eigenschaften" aus.

4. Klicken Sie im Bereich "Eigenschaften" auf die Registerkarte "Audit-Pfade".

   Die Registerkarte "Audit-Pfade" zeigt folgende Informationen für alle Datensätze an:

   - Letzte Aktualisierung:
   - Anwendername
   - Aktionstyp

   Hinweis: Die Spalte "Version" ist auch verfügbar, wird aber nicht standardmäßig angezeigt. Weitere Informationen finden Sie unter Schritt 5.

5. (Optional) Um die Audit-Pfade in einer bestimmten Spalte zu sortieren, wählen Sie "Aufsteigend sortieren" oder "Absteigend sortieren" aus der Drop-down-Liste der Zielspalte aus.

   Um zum Beispiel einen bestimmten Anwender zu überwachen, aktivieren Sie eine Sortierungsoption in der Drop-down-Liste der Spalte "Anwendername", und scrollen Sie dann zum entsprechenden Datensatz.

6. (Optional) Geben Sie an, welche Spalten das Produkt anzeigt:

   a. Wählen Sie "Spalten" aus einer Drop-down-Liste der Spalte aus.

   b. Deaktivieren Sie (Ausblenden) oder aktivieren Sie (Einblenden) nach Bedarf die Kontrollkästchen der Spalten.

   Um zum Beispiel die Spalte "Version" anzuzeigen, aktivieren Sie das Kontrollkästchen "Version" im Menü "Spalten".

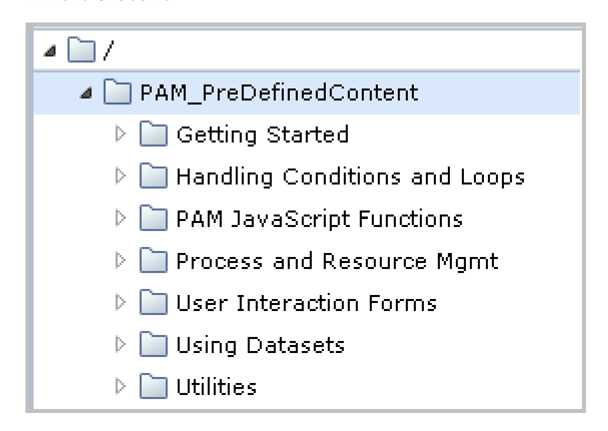
7. Prüfen Sie die Datensätze im Audit-Pfad.

Kapitel 16: Verwalten von Bibliotheksobjekten

Dieses Kapitel enthält folgende Themen:

Erstellen und Verwalten von Ordnern

Die Bibliothek eines neu installierten CA Process Automation-Domänen-Koordinationsrechners enthält keine Ordner im Navigationsbereich der Registerkarte "Bibliothek". Wenn Sie den standardmäßigen Inhalt auf der Startseite installieren, werden in der Bibliothek Ordner für vordefinierten Inhalt erstellt.



Normalerweise richtet ein Administrator die Ordnerstruktur für den Inhalt ein, der von Inhaltsdesignern erstellt wird. Designer speichern alle Automatisierungsobjekte in den Bibliotheksordnern. (Standardmäßig können Mitglieder der Designer-Gruppe Ordner erstellen.)

Hinweis: Für einen aktualisierten CA Process Automation werden alle Ordner in ihrer früheren Struktur mit ihren Inhalten migriert.

Einrichten von Ordnern für das Design

Sie können Ordner mit dem folgenden Prozess einrichten:

1. Planen der Ordnerstruktur (siehe Seite 372).
2. Erstellen von Ordnern (siehe Seite 374).
3. Gewähren von Ordnerzugriff (siehe Seite 374).

Planen der Ordnerstruktur

Als neuer CA Process Automation-Administrator müssen Sie zunächst entscheiden, wie Sie die Ordner auf der Registerkarte "Bibliothek" organisieren und verwenden möchten. Die Ordnerstruktur kann so tief sein, wie Sie es als praktisch empfinden.

Um die Aufgabe zur Exportvorbereitung einfacher zu gestalten, richten Sie vor Beginn der Designaktivitäten eine ähnliche Ordnerstruktur ein. Erstellen Sie auf der Stammebene der Bibliothek jeweils einen Ordner für alle Prozesse, die Sie automatisieren möchten. Erstellen Sie unter Verwendung Ihrer eigenen Namenskonventionen unter jedem Ordner auf Prozessebene einen Ordner auf Versionsebenen für die erste Release-Version. Wenn Sie Aktualisierungen für einen Prozess erstellen, können Sie weitere Ordner für die nachfolgenden Release-Versionen hinzufügen.

```
/ (Stammordner)
Automatisierter Prozess1
   Release-Version 1
   Release-Version 2
Automatisierter Prozess 2
   Release-Version 1
   Release-Version 2
```

Wenn Sie die erste Release-Version des ersten Prozesses, den Sie automatisieren, bereitstellen, exportieren Sie den Ordner der Release-Version, der alle in dieser Version enthaltenen Objekte enthält.

Berücksichtigen Sie beim Erstellen einer Ordnerstruktur die folgenden Vorgehensweisen:

- Erstellen Sie die Exportstruktur von null auf, und verwenden Sie den Ordner der Release-Version als Arbeitsordner. Inhaltsdesigner erstellen, aktualisieren und testen Objekte innerhalb des Ordners einer Release-Version oder eines seiner Unterordner. Jede Art der in diesem Schritt erstellten und exportierten Ordnerstruktur wird nach dem Import in der Produktionsumgebung reproduziert.
- Erstellen Sie Arbeitsordner. Wenn die erste Release-Version eines Prozesses für die Bereitstellung vorbereitet ist, erstellen Sie den Exportordner, und füllen Sie ihn mit den Objekten auf, die zur Release-Version gehören.
- Hybride Vorgehensweise. Erstellen Sie die Exportstruktur und verwenden Sie den Exportordner als Arbeitsordner für die bevorstehende Release-Version, bewahren Sie Objekte, die von mehreren Prozessen genutzt werden, jedoch in einem anderen Ordner auf Stammebene auf. Zum Beispiel können mehrere Prozesse benannte Datensätze und bestimmte Unterprozesse gemeinsam nutzen. Kalender können zeitplanübergreifend gemeinsam genutzt werden. Globale Ablaufpläne können gemeinsam genutzt werden. Kopieren Sie dann als Teil der Exportvorbereitung die erforderlichen Objekte aus dem Ordner der gemeinsam genutzten Objekte in den Exportordner.

Hinweis: Wenn Sie Ordner mit absoluten Pfaden exportieren, wird die vollständige Ordnerstruktur des Exportordners in der Produktionsumgebung reproduziert, wenn Inhalte importiert werden.

Erstellen von Ordnern

Sie erstellen einen Ordner im linken Bereich der Registerkarte "Bibliothek". Der linke Bereich ist der Navigationsbereich für die Bibliothek. Ein Ordner enthält den Inhalt, den Inhaltsdesigner anhand von Automatisierungsobjekten entwerfen. Alle Objekte, die einen bestimmten automatisierten Prozess unterstützen, müssen sich für den Import im gleichen Ordner oder der gleichen Ordnerstruktur befinden. Es ist günstig, für jedes Projekt einen Ordner auf Stammebene zu erstellen.

Innerhalb eines Ordners auf Prozessebene können Sie Unterordner erstellen. Beim Export darf der Ordner, den Sie als vordefinierten Inhalt exportieren, keine nicht verwendeten oder veralteten Objekte enthalten. Die Ordnerstruktur, die Sie für ein Projekt in der Designumgebung festlegen, wird nach dem Import in der Produktionsumgebung reproduziert.

Gehen Sie folgendermaßen vor:

1. Legen Sie die Stufe fest, auf der sich der Ordner befinden soll.

   Sie können unter dem Stammknoten oder unter einem vorhandenen Ordner einen Ordner erstellen.

2. Klicken Sie mit der rechten Maustaste auf den übergeordneten Knoten für den Ordner, und wählen Sie Neues Objekt, Ordner aus.

   Der Ordnerpfad wird im Hauptbereich mit einem Feld für den Namen angezeigt. Der Standardname wird als Ordner angezeigt.

3. Klicken Sie auf das Feld Name, löschen Sie den Standardordnernamen, und geben Sie einen Namen für diesen neuen Ordner ein.

So gewähren Sie Ordnerzugriff:

Administratoren (Mitglieder der PAMAdmins-Gruppe) haben Zugriff auf alle Ordner und auf die Inhalte aller Ordner.

Sie können Anwendern, die keine Administratoren sind, auf folgende Weisen Zugriff auf Ordner gewähren:

- Festlegen des Ordnerverantwortlichen (siehe Seite 375).

  Derjenige, der den Ordner (oder das Automatisierungsobjekt) erstellt, ist der erste Verantwortliche. Wenn Sie (als Administrator) alle Ordner erstellen, ist "Verantwortlichen festlegen" die einfachste Methode, um Anwendern, die keine Administratoren sind, Ordnerzugriff zu gewähren.

- Erstellen von Richtlinien für die einzelnen Inhaltsdesigner (siehe Seite 375).

  Sie können Inhaltsdesignern (Mitgliedern von PAMUsers oder einer anwenderspezifischen Gruppe), denen keine Inhaltsadministratoren-Rechte gewährt wurden, Zugriff auf bestimmte Ordner gewähren.

Festlegen des Ordnerverantwortlichen

Nur ein Inhaltsadministrator oder der Ordnerverantwortliche kann den Verantwortlichen eines Ordners ändern. Standardmäßig ist der Ersteller des Ordners für den Ordner verantwortlich. Der Verantwortliche hat unbegrenzte Berechtigungen für den Ordner. Als Inhaltsadministrator können Sie einen Ordner erstellen und dann die Ordnerverantwortung an die entsprechende Anwender-ID übertragen. Zum Beispiel können Inhaltsdesigner eigene Ordner haben, während der Ordner, der verwendet wird, um eine Release-Version als vordefinierten Inhalt zu exportieren, einem Administrator zugewiesen ist.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf Koordinationsrechner, und wählen Sie die geeignete *Koordinationsrechner-Umgebung* aus.
3. Wählen Sie einen Ordner aus.
4. Klicken Sie auf Verantwortlichen festlegen.
5. Geben Sie die Anwender-ID des Anwenders ein, der als Verantwortlicher festgelegt werden soll, und klicken Sie auf "Suchen".

   Hinweis: Die Suchergebnisse enthalten alle Anwender mit einer Anwender-ID oder einem Anwendernamen, die bzw. der die von Ihnen eingegebene Zeichenfolge enthält.
6. Wählen Sie den Anwender aus der angezeigten Liste aus.
7. Klicken Sie auf Speichern und Schließen.

Hinweis: Der Ordnereigentümer hat Zugriff auf den Ordner und kann ihn einzeln oder als vordefinierten Inhalt exportieren. Mit einer CA EEM-Richtlinie haben Sie mehr Kontrolle über die Aktionen, die ein Inhaltsdesigner auf einem Ordner ausführen kann.

Erstellen einer Richtlinie für jeden Inhaltsdesigner

Sobald Ihre Ordnerstruktur vorliegt und Ihre Inhaltsdesigner Anwenderkonten haben, können Sie diesen Designern Ordnerzugriff erteilen. Mit dem Ordnerzugriff wird der Ordner festgelegt, in dem ein Anwender oder eine Anwendungsgruppe Automatisierungsobjekte erstellen und steuern kann. Für diesen Vorgang müssen Sie jedem Inhaltsdesigner einen separaten Ordner zuweisen, und diese Ordner müssen sich direkt unter dem Stammordner befinden.

Eine auf Objekten basierte anwenderspezifische Richtlinie ermöglicht es Ihnen, angegebenen Anwendern oder Gruppen Ordnerzugriff zu erteilen. Zu den verfügbaren Zugriffsrechten für Ordner gehören "Liste", "Lesen", "Bearbeiten", "Löschen" und "Admin". Nachdem Sie die erste Richtlinie erstellt haben, können Sie diese Richtlinie als Vorlage für das Erstellen anderer Richtlinien verwenden.

Gehen Sie folgendermaßen vor:

1. Navigieren Sie zu CA EEM, und melden Sie sich an (siehe Seite 46).
2. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".
3. Klicken Sie auf "Neue Zugriffsrichtlinie für Objekt".

   Es wird eine neue Zugriffsrichtlinie angezeigt, bei der der Name der Ressourcenklasse "Objekt" ist.

4. Geben Sie einen Namen für diese Richtlinie ein, die einem bestimmten Inhaltsdesigner Ordnerzugriff gewährt.
5. Klicken Sie auf die Verknüpfung "Identitäten suchen", und klicken Sie auf "Suchen".
6. Wählen Sie den Namen des Inhaltsentwicklers aus, und klicken Sie auf den rechten Pfeil.

   Der Name wird in der Liste "Ausgewählte Identitäten" beginnend mit "[Anwender]" angezeigt.

7. Geben Sie Pfad und Namen des Ordners ein, den Sie für diesen Inhaltsdesigner im Feld "Ressource hinzufügen" erstellt haben, und klicken Sie auf "Ressource hinzufügen".

   Ihre Eingabe wird in der Ressourcen-Liste angezeigt.

8. Wählen Sie jede Berechtigung aus, die Sie diesem Inhaltsdesigner gewähren möchten. Gewähren Sie zum Beispiel alle Aktionen außer "Object_Admin".
9. Klicken Sie auf "Speichern".

   Die gespeicherte Richtlinie ähnelt dem folgenden Beispiel:

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Folder Access for Content Designer 1 Grants Content Designer 1 access to the /ContentDesigner1 folder	Object	Explizite Genehmigung	content designer 1	Object_List Object_Read Object_Edit Object_Delete	/ContentDesigner1

10. Testen Sie den Zugriff.
    a. Melden Sie sich mit den Anmeldeinformationen für diesen Anwender bei CA Process Automation an.
    b. Überprüfen Sie, dass der einzige Ordner, den Sie verwenden können, derjenige ist, für den Sie Zugriff gewährt haben.
11. Erstellen Sie auf einem der folgenden Wege für jeden zusätzlichen Inhaltsdesigner eine Richtlinie:
    - Wiederholen Sie die Schritte 2-10.
    - Öffnen Sie die gespeicherte Richtlinie, klicken Sie auf "Speichern unter", geben Sie einen neuen Namen ein, und bearbeiten Sie sie.

Hinweis: Um Lesezugriff auf alle Ordner zu gewähren, erstellen Sie eine Richtlinie mit Objekt, der Sie alle Inhaltsdesigner hinzufügen. Wählen Sie für den Stammordner "Object_List" und "Object_Read" aus.

So verwalten Sie Ordner:

Um Ordner zu verwalten, verwenden Sie eine Kombination der folgenden Vorgänge:

- Sichern aller Ordner und ihrer Inhalte (siehe Seite 384).
- Löschen von Ordnern (siehe Seite 385).
- Exportieren von Ordnern (siehe Seite 379).
- Importieren von Ordnern (siehe Seite 381).
- Verschieben von Ordnern (siehe Seite 378).
- Durchsuchen der Ordnerstruktur (siehe Seite 377).
- Anzeigen der Inhalte eines Ordners (siehe Seite 378).

Hinweise:

- Weitere Informationen über das Exportieren eines Ordners als Inhaltspaket finden Sie unter "Vorbereiten der Produktionsumgebung für eine neue Version (siehe Seite 388)".
- Weitere Informationen über das Löschen und Wiederherstellen von gelöschten Ordnern finden Sie unter "Verwenden des Papierkorbs (siehe Seite 405)".

Durchsuchen der Ordnerstruktur

Sie können anhand eines Ordnernamens, der mit der Zeichenfolge oder der Teilzeichenfolge anfängt, die Sie angeben, nach Ordnern suchen. Das Suchfeld befindet sich am oberen Rand im linken Bereich der Registerkarte "Bibliothek".

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf "Koordinationsrechner", und wählen Sie die entsprechende *Koordinationsrechnerumgebung aus*.
3. Geben Sie den Namen oder einen Teil des Namens für einen Ordner oder für einen Ordnersatz im Suchfeld ein.
4. Prüfen Sie die gefilterte Liste. Sie werden feststellen, dass der Ordner am Ende jeden Pfads in der angezeigten Liste Ihren Suchkriterien entspricht.

Anzeigen der Inhalte eines Ordners

Wählen Sie einen Ordner aus, um seine Inhalte anzuzeigen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf "Koordinationsrechner", und wählen Sie die entsprechende *Koordinationsrechnerumgebung aus*.
3. Navigieren Sie durch die Ordnerstruktur, und erweitern Sie je nach Bedarf die Ordner. Oder geben Sie Suchkriterien in das Suchfeld ein, um die angezeigte Liste nach Ordnern zu filtern, die mit dem von Ihnen eingegebenen Namen anfangen.
4. Wenn der Zielordner angezeigt wird, wählen Sie ihn aus.

   Die Ordnerinhalte werden in Tabellenform im Hauptbereich angezeigt.
5. (Optional) Zeigen Sie die Daten in der gewünschten Reihenfolge an. Klicken Sie auf die Kopfzeile der Spalte, nach der Sie die Tabelle sortieren möchten, und wählen Sie "Aufsteigend" oder "Absteigend".

Verschieben eines Ordners

Sie können Ordner in einer Koordinationsrechner-Bibliothek verschieben.

Hinweis: Um einen Ordner von einer Koordinationsrechner-Bibliothek in eine andere zu verschieben, exportieren Sie den Ordner (siehe Seite 379).

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf "Koordinationsrechner", und wählen Sie die *Koordinationsrechner-Umgebung* mit der Bibliothek aus, die den Quellordner enthält.
3. Navigieren Sie durch die Ordnerstruktur, und erweitern Sie je nach Bedarf die Ordner.

   Hinweis: Geben Sie einen Teil des Ordnernamens ein, um Ordner mit Namen anzuzeigen, die mit der eingegebenen Zeichenfolge beginnen.

4. Wenn der Zielordner angezeigt wird, wählen Sie ihn aus, und klicken Sie auf "Ausscheiden".

5. Navigieren Sie zum Zielordner, und klicken Sie dann auf "Einfügen".

   Eines der folgenden Ereignisse tritt auf:

   - Wenn der Zielordnername sich vom Quellordnernamen unterscheidet, fügt der Koordinationsrechner den Quellordner als einen Unterordner des Zielordners hinzu.

   - Wenn der Zielordner und der Quellordner den gleichen Namen haben, fügt der Koordinationsrechner den Inhalt des Quellordners zum Zielordner hinzu. Das heißt, der Koordinationsrechner führt die Inhalte der beiden Ordner zusammen.

Exportieren von Ordnern

Wenn Sie eine der folgenden Elemente exportieren, erstellt das Produkt eine XML-Datei, die Sie importieren können:

- Ein Objekt.

- Ein Ordner, der mehrere Objekte enthält, die im Ziel-Koordinationsrechner benötigt werden. Die Objekte können nicht zugehörig zueinander sein, möglicherweise für verschiedene Prozesse. Der Wert der Release-Version ist nicht anwendbar.

- Ein Ordner, der alle Objekte enthält, bei denen es sich um eine Release-Version eines Prozesses handelt. Vor dem Exportvorgang definieren Sie eine Release-Version für den Ordner und für jedes Objekt im Ordner.

  Hinweis: Weitere Informationen finden Sie unter "Szenario: Vorbereiten eines Ordners für das Exportieren als vordefinierter Inhalt".

Inhaltsadministratoren und Inhaltsdesigner können einen Ordner aus dem Bibliotheksbrowser in eine Exportdatei auf dem lokalen Host exportieren. Die Exportdatei behält den Pfad zum Ordner und die hierarchische Struktur von Objekten und untergeordneten Ordnern bei.

Administratoren können einen Ordner folgendermaßen exportieren:

Exportieren, {Absolute Pfade | Relative Pfade}

Beim änderbaren Export können die Empfänger in der Zielumgebung die exportierten Objektversionen im Ordner aktualisieren.

Als vordefinierten Inhalt exportieren, {Absolute Pfade | Relative Pfade}

Beim nicht änderbaren Export können die Empfänger in der Zielumgebung die exportierte Version der Objekte und die Beschriftung der Release-Version nicht aktualisieren.

Hinweis: Sie können keine Objekte exportieren, die sich in mehreren Ordnern als Verknüpfungen in einem Paket befinden. Erstellen Sie stattdessen einen Exportordner, und stellen Sie dann alle Objekte für den Export in diesem Ordner zusammen. Weitere Informationen finden Sie im *Handbuch für Inhaltsdesign*.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf "Koordinationsrechner", und wählen Sie die geeignete *Koordinationsrechner-Umgebung* aus.
3. Navigieren Sie zum Ordner, der exportiert werden soll, klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie eine der folgenden Optionen aus:
   - Exportieren, Absolute Pfade
   - Exportieren, Relative Pfade
4. Um die XML-Datei zu speichern, klicken Sie im Dialogfeld zum Herunterladen der Datei auf "Speichern".

   Hinweis: Der Standarddateiname lautet *folder-name*.xml.
5. Navigieren Sie auf Ihrem lokalen Laufwerk zum Speicherort, wo die XML-Datei gespeichert werden soll.
6. Definieren Sie den Namen, unter dem die Datei gespeichert werden soll.

   Hängen Sie beispielsweise "_RP" an den Dateinamen an, um auf einen relativen Pfad hinzuweisen, bzw. "_AP" bei einem absoluten Pfad.

   *Ordnername*_RP.xml

   *Ordnername*_AP.xml
7. Klicken Sie auf "Speichern".

   Das Produkt exportiert den Ordner und die zugehörigen Inhalte.

Importieren von Ordnern

Inhaltsadministratoren können die XML-Datei importieren, die einen exportierten Ordner und die darin enthaltenen Objekte darstellt. Wenn der Ordner mit dem absoluten Pfad exportiert wurde, wird die hierarchische Struktur von Objekten und untergeordneten Ordnern in der Exportdatei beibehalten. Wenn der Ordner mit dem relativen Pfad exportiert wurde, wird die Struktur des Exportordners im Importordner erstellt.

Der Importprozess ist der gleiche, unabhängig davon, auf welche Weise der Inhalt exportiert wurde. Die jeweils anwendbaren Optionen basieren auf dem Inhalt der Exportdatei.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf Koordinationsrechner, und wählen Sie die *Koordinationsrechner-Zielumgebung* aus.
3. Navigieren Sie zum Zielordner für das Importieren.
4. Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie Importieren aus.
5. Führen Sie die folgenden Vorgänge im Dialogfeld "Importieren" aus:
    a. Klicken Sie auf Durchsuchen, und navigieren Sie zum Speicherort der exportierten Datei auf Ihrem lokalen Laufwerk.
    b. Wählen Sie die exportierte XML-Datei aus, und klicken Sie auf Öffnen.

c. Wählen Sie aus, wie ein Objekt importiert werden soll, das denselben Namen wie ein vorhandenes Objekt im gleichen Pfad hat. Ziehen Sie dabei Ihr Wissen über die Objekte, die im Importordner vorhanden sind, heran.

Importieren

Behandeln Sie die importierte Objektversion als neue Version des vorhandenen Objekts. Wählen Sie diese Option aus, wenn der Zweck dieses Imports ein Upgrade ist und Sie die Historie der Vorgängerversionen behalten möchten. Wenn das importierte Objekt die gleiche Release-Version hat, wird die vorhandene Release-Version mit der Release-Version des importierten Objekts überschrieben.

Die Release-Version des importierten Objekts wird überschrieben, wenn ein ähnliches Objekt mit der gleichen Release-Version vorhanden ist.

Nicht importieren

Beenden Sie den Import des Objekts, und behalten Sie das vorhandene Objekt. Wenn Sie diese Option auswählen, listet der Importprozess die Objekte mit Konflikt verursachenden Namen auf. Wenn Konflikte auftreten, können Sie den Importvorgang erneut durchführen und in einen leeren Ordner importieren. Alternativ können Sie das Objekt in der Quellumgebung umbenennen und dann den Export und Import wiederholen. Diese Option ist eine gute Wahl, wenn die zu importierenden Objekte neue Objekte sind und keine neuen Versionen von vorhandenen Objekten.

Importieren und ersetzen

Löschen Sie das vorhandene Objekt, und importieren Sie die neue Version des Objekts als Version 0.

d. Wählen Sie aus, ob die Version der Objekte im Importordner als aktuelle Version festgelegt werden soll. Die aktuelle Version des Prozesses ist die Version, die ausgeführt wird, wenn der Prozess startet. Diese Version wird nach dem Import aktiv. Andere Prozesse können die Objekte auch verwenden, die dieser Prozess verwendet. Wenn die importierten Versionen bereits als aktuelle Version festgelegt sind, dann sind sie sofort zur Verwendung verfügbar. Weitere Informationen finden Sie unter Bestimmen, ob als aktuelle Version importiert werden soll (siehe Seite 395).

e. Wählen Sie aus, ob anwenderspezifische Operatoren zur Verfügung gestellt werden sollen.

f. Wählen Sie aus, ob die anwenderspezifische Operatorgruppe auf der Registerkarte "Module" für die Domäne veröffentlicht werden soll.

Hinweis: Veröffentlichen Sie keine anwenderspezifische Operatorgruppe, außer, der Ordner, den Sie importieren, gehört zu einer anderen Domäne.

6. Klicken Sie auf Senden, um den Importprozess zu starten.

7. Klicken Sie in der Meldung zur Verifizierung eines erfolgreichen Imports auf OK.
8. Sie können den importierten Ordner und dessen Inhalte im gegenwärtig angezeigten Ordner überprüfen. Beachten Sie folgende Ergebnisse:
   - Wenn Sie den Ordner als vordefinierten Inhalt exportiert haben:
     - Sie können den Attributwert "Release-Version" für Objekte oder für das Paket mit vordefiniertem Inhalt nicht ändern.
     - Sie können die importierte Version von Objekten nicht ändern. Objekte werden während des Imports als Baseline-Version erstellt.
   - Wenn Sie ausgewählt haben, dass während dem Importieren anwenderspezifische Operatoren zur Verfügung gestellt werden, sind die importierten anwenderspezifischen Operatoren zur Verwendung verfügbar.
   - Wenn Sie die anwenderspezifische Operatorgruppe in der Registerkarte "Module" veröffentlicht haben, konfigurieren Sie Werte für die anwenderspezifische Operatorgruppe (siehe Seite 324).

Sichern aller Ordner und ihrer Inhalte

Sie können eine Bibliothek aus Ordnern und deren Inhalt sichern, um sich vor Verlusten zu schützen. Initiieren Sie einen Export auf Stammebene der Ordnerstruktur. Der Exportprozess erstellt eine XML-Datei mit allen Informationen, die benötigt werden, um die Bibliotheksordner und ihren Inhalt nach dem Import wiederherzustellen. Die Best Practice für Sicherheitszwecke besteht darin, diese XML-Datei an einem anderen Standort aufzubewahren. Wenn Sie Ihre Bibliothek verlieren, können Sie sie jederzeit rekonstruieren, indem Sie die XML-Datei in das Stammverzeichnis eines neuen Koordinationsrechners importieren.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf "Koordinationsrechner", und wählen Sie die geeignete *Koordinationsrechner-Umgebung* aus.
3. Klicken Sie mit der rechten Maustaste auf den Stammordner, und wählen Sie die Option "Exportieren".
4. Entscheiden Sie dann, ob Sie den vollständigen Pfad für die exportierten Objekte oder den Pfad relativ zu einem Ordner, der das Objekt enthält, einschließen möchten.
5. Klicken Sie auf "Exportieren", und wählen Sie einen der folgenden Pfadtypen aus:
   - Absolute Pfade.
   - Relative Pfade.

   Auf Windows-Hosts wird das Dialogfeld "Datei herunterladen" geöffnet. Sie können auswählen, ob Sie die Datei öffnen oder speichern möchten.
6. Wählen Sie "Speichern" aus.

   Auf Windows-Hosts wird das Dialogfeld "Speichern unter" geöffnet.
7. Geben Sie den Dateinamen an, mit dem die XML-Datei und der Pfad gespeichert werden sollen. Zum Beispiel: librarybackup_*date*.xml
8. Klicken Sie auf "Speichern".

Löschen von Ordnern

Sie können einen Ordner löschen, den Sie nicht mehr benötigen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf "Koordinationsrechner", und wählen Sie die entsprechende *Koordinationsrechnerumgebung aus*.
3. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie "Löschen" aus.
   - Wählen Sie den Ordner aus, und klicken Sie in der Symbolleiste auf die Schaltfläche "Löschen".

   Es wird eine Bestätigungsmeldung für den Löschvorgang angezeigt.
4. Klicken Sie auf "Ja".

   Der Ordner wird gelöscht.

   Hinweis: Der Papierkorb enthält sowohl gelöschte Automatisierungsobjekte als auch gelöschte Ordner. Wenn ein Automatisierungsobjekt wiederhergestellt wird, werden die gelöschten Ordner im ursprünglichen Ordnerpfad auch wiederhergestellt.

So verwalten Sie Automatisierungsobjekte:

Administratoren verwenden die Bibliothek, um Automatisierungsobjekte innerhalb einer Ordnerstruktur zu verwalten. Im Folgenden finden Sie Wartungsaufgaben:

- Festlegen eines neuen Verantwortlichen für Automatisierungsobjekte (siehe Seite 387).
- Hinzufügen von Tags zur Verwendung in Objektsuchen.
- Verwalten von Objektversionen.
- Löschen von Automatisierungsobjekten aus einer Ordnerstruktur.
- Verschieben eines Objekts in einen anderen Ordner.
- Kopieren eines oder mehrerer Objekte zu einem Koordinationsrechner in derselben Umgebung.

  Weitere Informationen finden Sie unter Exportieren eines einzelnen Objekts und Importieren eines einzelnen Objekts.

  Weitere Informationen finden Sie unter Exportieren von Ordnern (siehe Seite 379) und Importieren von Ordnern (siehe Seite 381).
- Kopieren von Objekten in eine abweichende Umgebung, zum Beispiel aus einer Designumgebung in eine Produktionsumgebung.

  Weitere Informationen finden Sie in Exportieren eines Ordners als vordefinierter Inhalt (siehe Seite 393) und Importieren von vordefiniertem Inhalt (siehe Seite 398).

Festlegen eines neuen Verantwortlichen für Automatisierungsobjekte

Nur ein Inhaltsadministrator oder der Verantwortliche eines Automatisierungsobjekts kann den Verantwortlichen eines Automatisierungsobjekts ändern. Standardmäßig entspricht der Verantwortliche eines Automatisierungsobjekts der zur Anmeldung verwendeten Anwender-ID desjenigen, der das Objekt erstellt. Der Verantwortliche eines Objekts hat unbegrenzte Berechtigungen für dieses Objekt. Als Verantwortlicher eines Automatisierungsobjekts oder als Inhaltsadministrator können Sie die Verantwortung an einen anderen CA Process Automation-Anwender übertragen. Sie können auch einen neuen Verantwortlichen für mehrere Objekte festlegen, für die Sie verantwortlich sind.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf "Koordinationsrechner", und wählen Sie die entsprechende *Koordinationsrechnerumgebung aus*.
3. Wählen Sie den Ordner aus, der die Zielautomatisierungsobjekte enthält.
4. Wählen Sie eine oder mehrere Zeilen im Raster für die Zielobjekte aus.
5. Klicken Sie auf "Verantwortlichen festlegen".
6. Geben Sie die CA Process Automation-Anwender-ID des neuen Verantwortlichen an.

Vorbereiten der Produktionsumgebung für eine neue Version

Inhaltsdesigner bereiten einen Ordner für das Exportieren als vordefinierter Inhalt vor.

Inhaltsadministratoren überprüfen, ob die als Ziel für Operatoren eingerichteten Kontaktpunkte dem Koordinationsrechner oder den Agenten in der Produktionsumgebung zugeordnet sind. Wenn die Inhaltsadministratoren die Überprüfung vor dem Importvorgang abschließen, können die Objekte als aktuelle Version importiert werden. Wenn sie die Überprüfung erst nach dem Importvorgang abschließen, werden die Objekte nicht als aktuelle Version importiert.

Der Anwender, der den Export und Import ausführt, überprüft, ob der Prozess in der Produktionsumgebung wie erwartet funktioniert. Anschließend können die Produktionsanwender die neue Version verwenden.

Die Übergabe umfasst die folgenden Schritten:

1. Exportieren und Importieren von Objekten in einem Paket mit vordefiniertem Inhalt (siehe Seite 390).
2. Konfigurieren von Produktionszielen für den neuen Prozess
3. Überprüfen, dass der Prozess einwandfrei funktioniert (siehe Seite 403)
4. Übergeben des neuen Prozesses an die Produktionsanwender

   Hinweis: Die Übergabe erfolgt außerhalb der CA Process Automation-Anwendung.

Informationen zum Exportieren und Importieren von vordefinierten Inhalten

Ein Paket mit vordefiniertem Inhalt wird aus einem Ordner erstellt, der Automatisierungsobjekte für eine bestimmte Version enthält. Normalerweise enthält der Ordner die folgenden Objekte:

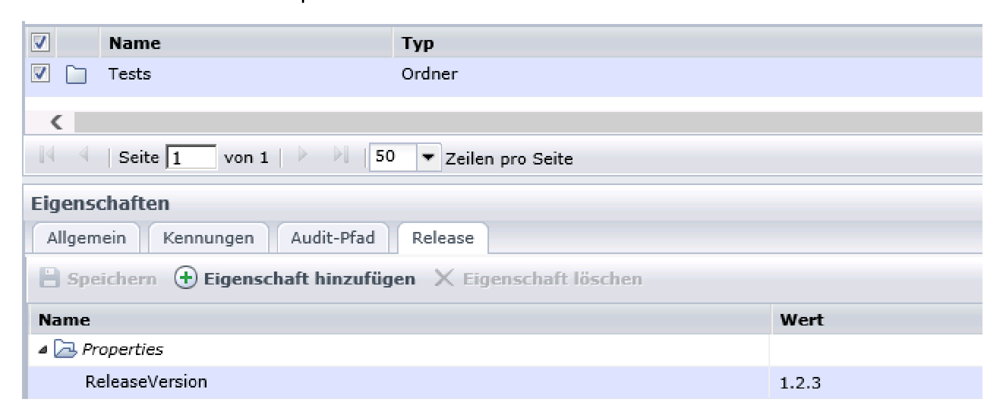
- Einen Prozess, entweder das erste Release oder ein späteres Release.
- Alle Objekte, die der Prozess verwendet.
- Alle Objekte, die erforderlich sind, damit Anwender den Prozess ausführen können.

Vor dem Export fügen Sie zum Ordner sowie allen Objekten einen eindeutigen Wert für die Release-Version hinzu und stellen sicher, dass aus jedem Objekt eine Baseline erstellt wurde. Durch die Baseline wird eine statische Version in der Designumgebung der einzelnen Objekte zum Zeitpunkt des Release erstellt.

Wenn Sie einen Ordner als vordefinierter Inhalt exportieren, erstellt CA Process Automation beim Import automatisch eine Baseline aus allen Objekten im vordefinierten Inhalt. Pakete mit vordefiniertem Inhalt und die Objekte, die sie enthalten, können in der neuen Umgebung nicht geändert werden. (Um ein Objekt in der Importumgebung ändern zu können, speichern Sie die Baseline-Version als neue Version.)

Beispiele für Release-Versionen

Die Registerkarte "Versionen" im folgenden Screenshot enthält die Eigenschaft "ReleaseVersion". Im Beispiel ist der Wert 1.2.3.



Das folgende Beispiel veranschaulicht die Registerkarte "Versionen" für einen Prozess, wobei der hinzugefügte Wert für "Release-Version" mit dem Wert, der für den Ordner hinzugefügt wurde, übereinstimmt.

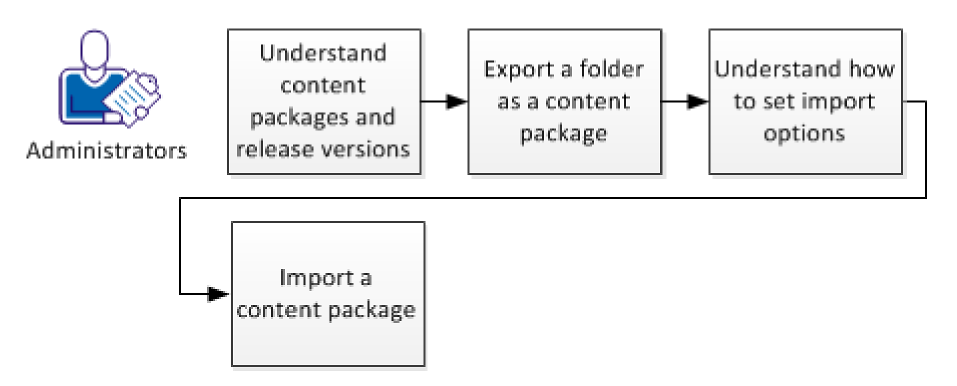


Beachten Sie, dass aus der Release-Version keine Baseline erstellt wurde. Die Schaltfläche " Baseline" ist aktiviert. Wenn Sie ein Objekt für ein Release finden, aus dem in der Quellumgebung keine Baseline erstellt wurde, erstellen Sie aus der Version für das Release eine Baseline.

Hinweis: Es besteht die Möglichkeit, mehrere Prozesse in einem Ordner gleichzeitig als vordefinierter Inhalt zu exportieren und das Attribut "Release-Version" zu verwenden, um die Ordnerinhalte zu beschreiben.

Exportieren und Importieren von Objekten in einem Paket mit vordefiniertem Inhalt

Verwenden Sie vordefinierte Inhalte, um einen Satz von zusammengehörenden Objekten, bei denen es sich um eine Release-Version handelt, von einem Koordinationsrechner zu einem anderen Koordinationsrechner zu exportieren und zu importieren. In den meisten Fällen befinden sich der Quell- und der Ziel-Koordinationsrechner in unterschiedlichen Umgebungen. Wenn Sie einen Ordner als vordefinierten Inhalt exportieren, erstellt der Exportprozess eine XML-Datei in Ihrem lokalen Laufwerk. Wenn Sie in einen anderen Koordinationsrechner importieren, wählen Sie diese XML-Datei aus Ihrem lokalen Laufwerk aus. Das importierte Ergebnis ist der vordefinierte Inhalt.



Gehen Sie folgendermaßen vor:

1. Machen Sie sich mit dem Zweck von vordefiniertem Inhalt und Release-Versionen vertraut. Sehen Sie sich die folgenden Themen an:
   - Informationen zu vordefiniertem Inhalt (siehe Seite 391)
   - Informationen zu Release-Versionen (siehe Seite 392)
2. Exportieren Sie einen Ordner als vordefinierter Inhalt (siehe Seite 393).
3. Machen Sie sich mit der Auswirkung vom Festlegen unterschiedlicher Importoptionen vertraut. Sehen Sie sich die folgenden Themen an:
   - Bestimmen, ob als aktuelle Version importiert werden soll (siehe Seite 395)
   - So legen Sie Importoptionen fest (siehe Seite 396)
4. Importieren von vordefiniertem Inhalt (siehe Seite 398).

Weitere Informationen:

Beispiel: Exportieren und Importieren von vordefinierten Inhalten (siehe Seite 401)

Informationen zu vordefiniertem Inhalt

Objekte können auf die folgenden Arten exportiert werden:

- Ein einzelnes Objekt
- Ein Ordner
- Ein Ordner als vordefinierter Inhalt

Das Exportieren eines Ordners als vordefinierter Inhalt unterscheidet sich folgendermaßen vom Exportieren eines Ordners:

- Der Wert für die Release-Version von einem beliebigen Objekt, das Sie in einem *Ordner als vordefinierter Inhalt* exportieren, kann nach dem Import nicht geändert werden. (Objekte, die in einem *Ordner* exportiert werden, benötigen keinen Wert für die Release-Version.)
- Der Wert für die Release-Version von einem Objekt, das Sie in einem Ordner als vordefinierter Inhalt exportieren, kann nach dem Import nicht geändert werden.

Exportieren Sie einen Ordner, wenn kein Bedarf besteht, zu seinen Objekten eine Release-Version zuzuweisen. Dies ist zum Beispiel der Fall, wenn Sie Objekte in einem Ordner von einem Design-Koordinationsrechner zu einem anderen Design-Koordinationsrechner exportieren.

Exportieren Sie einen Ordner als vordefinierten Inhalt, wenn Sie Objekte aus einer Designumgebung in eine Produktionsumgebung exportieren. Normalerweise stellen die Objekte in einem Paket mit vordefiniertem Inhalt ein Release eines automatisierten Prozesses dar. In diesem Fall besteht Bedarf, die Version der einzelnen Objekte zum Zeitpunkt des Release zu bewahren. Das Inhaltspaket enthält:

- Die Release-Version des Prozessobjekts.
- Alle Objekte, die der Prozess verwendet.
- Alle Objekte, die Produktionsanwender verwenden, um den Prozess zu starten oder um mit dem Prozess zu interagieren.

Ein Paket mit vordefiniertem Inhalt ist eine eigenständige Einheit. Ein Paket mit vordefiniertem Inhalt enthält einen Ordner mit Objekten, die zusammen für den Export gepackt werden. Vor dem Export wird die Version von jedem Objekt, das exportiert wird, mit einem Wert für die Release-Version gekennzeichnet. Der gleiche Wert wird dem Ordner als Release-Version zugewiesen.

Der Importprozess stellt alle Objekte im Paket mit vordefiniertem Inhalt für die Bibliothek bereit. Wenn sie als aktuell importiert wurden, dann steht das Objekt für die Verwendung zur Verfügung. Anwender in der Importumgebung können die Werte für "Release-Version" nicht erstellen oder ändern.

Der Importprozess für vordefinierten Inhalt erstellt für jedes Objekt eine Baseline. Die Absicht besteht darin, die Release-Version der Objekte unverändert zu verwenden. Allerdings ist es möglich, ein importiertes Objekt als neue Version zu speichern, das Objekt zu ändern und das geänderte Objekt als aktuelle Version zu speichern. In diesem Fall bleibt die Baseline-Version mit dem Wert für die Release-Version unverändert. Dadurch wird verhindert, dass diese Objekte in einer potenziell schädlichen Weise geändert werden. Um unerwünschte Änderungen umzukehren, legen Sie die Baseline-Version als aktuelle Version fest. Die Inhaltsdesigner, die die Fehlerbehebung durchführen, können nicht änderbare Objektversionen identifizieren, die zur Produktionsumgebung importiert wurden.

Wenn Sie ein Objekt von einem Drittanbieter in eine Designumgebung, die Sie ändern möchten, importieren, dann erstellen Sie eine Kopie aus diesem Objekt. Sie können die Objektkopie dann aktualisieren, und Sie können eine andere Release-Version zuweisen.

Informationen zu Release-Versionen

Bevor Sie einen Ordner als Paket mit vordefiniertem Inhalt exportieren, der einen Prozess und die enthaltenen Objekte umfasst, führt der Inhaltsdesigner die folgenden Aktionen aus:

- Festlegen der Release-Version aller Objekte
- Festlegen der Release-Version des Ordner, der das oder die Objekt(e) enthält

Nach dem Import haben Objekte die gleichen Release-Versionswerte, die Sie exportiert haben. Wenn Sie einen Ordner als vordefinierter Inhalt exportieren, befindet sich das importierte Paket im nicht änderbarem Modus. Die Zielanwender können den Wert der Release-Version, den Sie für diese Version festlegen, nicht ändern. Der Wert der Release-Version unterstützt Inhaltsdesigner, die in der Designumgebung arbeiten, eine bestimmte Version eines Objekts in der Produktionsumgebung zu identifizieren.

Hinweis: CA Process Automation legt die Sperre für das Release-Versionsattribut sowohl für das Objekt als auch die freigegebene Objektversion fest. Aus diesem Grund können Anwender den Wert der Release-Version für die importierte Objektversion nicht ändern und keine Werte für die Release-Version für neue Objektversionen festlegen.

Anwender können nach dem Import nicht änderbare Werte für die Release-Version nicht ändern. Erwägen Sie den Bedarf an Release-Versionen basierend auf den Aktionen, die Sie mit den Objekten durchführen. Zum Beispiel:

- Wenn Sie von einer *Designumgebung* in eine andere exportieren, legen Sie (optional) Attributwerte für die Release-Version fest, und exportieren Sie den Ordner.
- Wenn Sie von einer Designumgebung in eine *Produktionsumgebung* exportieren, müssen Inhaltsdesigner Attributwerte für die Release-Version für alle Objekt sowie den Ordner, in dem sie sich befinden, festlegen. Designer exportieren diesen Ordner dann als vordefinierten Inhalt.

Die folgenden Regeln bestimmen den Export und Import von Release-Versionen:

- Wenn eine der folgenden Aussagen wahr ist, sind Release-Versionen beim Importieren nicht änderbar:
  - Die Objekte sind in einem Paket mit vordefiniertem Inhalt enthalten.
  - Die Release-Version des Objekts war vor dem Exportieren nicht änderbar.
- CA Process Automation erstellt Baselines aus importierten Versionen, wenn Objekte als vordefinierter Inhalt (mit nicht änderbaren Release-Versionen) importiert werden.

  Hinweis: Wenn ein Objekt erneut mit der gleichen Release-Version importiert wird, wird dieses Objekt überschrieben.

Die folgenden Regeln bestimmen das Kopieren und Einfügen von importierten Objekten:

- Die erste Version der Objektkopie behält den Wert der Release-Version und die Festlegung, ob sie änderbar ist, bei.
- Wenn die aktuelle Version des ursprünglichen Objekts als Baseline festgelegt ist und das Attribut "Release Version" des Objekts nicht änderbar ist, wird die Objektkopie auch als Baseline festgelegt.

Exportieren eines Ordners als vordefinierter Inhalt

Inhaltsdesigner bereiten Objekte, die zur gleichen Release-Version zugeordnet sind, für den Export vor. Anschließend exportiert ein Inhaltsdesigner oder ein Administrator das Paket mit dem vordefinierten Inhalt. Der folgende Vorgang umfasst sowohl den Vorbereitungs- als auch den Exportschritt.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Bibliothek.
2. Klicken Sie auf Koordinationsrechner, und wählen Sie die *Koordinationsrechner-Quellumgebung* aus.

3. Navigieren Sie zum Zielordner. Stellen Sie sicher, dass der Ordner alle Objekte enthält, die Sie exportieren wollen. Stellen Sie sicher, dass der Ordner nur die Objekte enthält, die Sie exportieren wollen.
4. Fügen Sie die Release-Version zum Zielordner hinzu:
    a. Wählen Sie im Navigationsbereich den Ordner aus, der den zu exportierenden Ordner enthält.
    b. Klicken Sie im Hauptbereich mit der rechten Maustaste auf den zu exportierenden Ordner, und wählen Sie Eigenschaften aus.
    c. Klicken Sie auf die Registerkarte Release.
    d. Doppelklicken Sie auf die Spalte Wert in der Zeile Release-Version.
    e. Geben Sie die Release-Version ins Dialogfeld Wert ein, und klicken Sie auf OK.
    f. Klicken Sie auf "Speichern".
5. Fügen Sie die Release-Version der ausgewählten Version der einzelnen Objekte im Zielordner hinzu, und stellen Sie sicher, dass aus der ausgewählten Version eine Baseline erstellt wurde.
    a. Wählen Sie den Zielordner aus, der die zu exportierenden Objekte enthält.
    b. Klicken Sie mit der rechten Maustaste auf ein Objekt, und wählen Sie Eigenschaften aus.
    c. Wählen Sie die Registerkarte Release aus.
    d. Klicken Sie mit der rechten Maustaste auf die Zeile der zu exportierenden Version, wählen Sie Release-Version festlegen aus, geben Sie den gleichen Wert für die Release-Version ein, den Sie dem Ordner zugewiesen haben, und klicken Sie auf OK.
    e. Wenn der Baseline-Wert für die ausgewählte Zeile "Nein" ist, klicken Sie auf die Registerkarte Versionen und anschließend auf Baseline. Klicken Sie zur Bestätigung der Baseline-Erstellung auf Ja.

       Hinweis: Es ist wichtig, vor dem Export Baseline-Objekte zu erstellen, damit Sie jederzeit über ein gespeichertes Image in der Designumgebung aller Objekte zum Zeitpunkt des Release verfügen. (Während des Importprozesses wird aus allen Objekten automatisch eine Baseline erstellt.)
    f. Klicken Sie auf OK.
    g. Wiederholen Sie diese Schritte für jedes Objekt im Ordner.

6. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf den Ordner, und aktivieren Sie eine der folgenden Optionen:

   - Als vordefinierten Inhalt exportieren, Absolute Pfade

     Enthält den vollständigen Pfad für den ausgewählten Ordner.

   - Als vordefinierten Inhalt exportieren, Relative Pfade

     Enthält den relativen Pfad bezogen auf den Ordner, der den ausgewählten Ordner enthält.

7. Speichern Sie die Datei des exportierten Pakets.

   a. Klicken Sie auf Speichern, um die XML-Datei zu speichern.

   b. Navigieren Sie zu einem Ordner auf Ihrem lokalen Laufwerk, und klicken Sie auf Speichern.

   c. Wenn das Dialogfeld "Download abgeschlossen" angezeigt wird, klicken Sie auf Schließen.

   CA Process Automation exportiert den vordefinierten Inhalt als XML-Datei. Der vordefinierte Inhalt kann in einen anderen Koordinationsrechner importiert werden. Die Datei *Dateiname*.xml ist verschlüsselt.

Bestimmen, ob als aktuelle Version importiert werden soll

Beim Importieren geben Sie an, ob Sie Objekte als aktuelle Version importieren möchten. Importieren Sie Objekte als aktuelle Version, wenn beide der folgenden Aussagen wahr sind:

- Alle Ziele sind als Kontaktpunkt, Proxy-Kontaktpunkt oder Kontaktpunktgruppe definiert.
- Sie haben Produktionsziele für den neuen Prozess konfiguriert.

Hinweis: Sie können einen Prozess als aktuelle Version importieren, wenn die Ziele Ausdrücke sind, die auf Variablen in einem Datensatz zeigen. Beim Importieren können Sie die Variablen im Datensatz ändern, damit sie auf Produktionskontaktpunkte verweisen.

Nur wenn Sie ein Ziel als Agent-ID, IP-Adresse oder Hostname definiert haben, erfordert CA Process Automation, dass Sie mit dem Zuordnen von Operatorzielen zu Produktionshosts warten, bis der Import abgeschlossen ist. Importieren Sie in diesem Fall keine Objekte als aktuelle Version. Aktualisieren Sie stattdessen die Ziele in den Operatoren nach dem Import, und markieren Sie dann die importierte Version als aktuelle Version.

So legen Sie Importoptionen fest

CA Process Automation bietet Ihnen einen gewissen Spielraum für Flexibilität beim Importieren von Objekten.



Wenn der Import anwenderspezifische Operatoren enthält, wählen Sie Importierte anwenderspezifische Operatoren verfügbar machen aus.

Wenn die anwenderspezifischen Operatoren neu sind und zu einer neuen anwenderspezifischen Gruppe gehören, führen Sie die Aktion durch, die zu Ihrer Umgebung passt.

- Wählen Sie Konfiguration der anwenderspezifischen Operatorgruppe veröffentlichen nicht aus, wenn sich die Importumgebung in derselben Domäne wie die Exportumgebung befindet. In diesem Fall ist die Konfiguration der anwenderspezifischen Operatorgruppe bereits veröffentlicht.
- Wählen Sie Konfiguration der anwenderspezifischen Operatorgruppe veröffentlichen aus, wenn sich die Importumgebung in einer anderen Domäne als die Exportumgebung befindet.

Berücksichtigen Sie den Importinhalt, wenn Sie Importierte Version als aktuelle Version festlegen konfigurieren, und wählen Sie aus, wie doppelte Namen verarbeitet werden sollen.

- Um die importierten Objekte zu aktivieren und bei Bedarf auf eine Vorgängerversion eines importierten Objekts zurückzusetzen:
  - Aktivieren Sie: Importieren
  - Aktivieren Sie: Importierte Version als aktuelle Version festlegen

  Hinweis: Diese Optionen sind ideal, wenn Sie eine Upgrade-Release-Version importieren und alle Operatorziele als Hosts in der Importumgebung festgelegt sind. Sie können erwarten, dass Sie über duplizierte Namen informiert werden, weil Objekte des letzten Release im Zielordner gefunden werden.

- Um zu importieren, ohne die Objekte, für die ein Upgrade durchgeführt wurde, zu aktivieren und den aktuellen Status der Vorgängerversion beizubehalten:
  - Aktivieren Sie: Importieren
  - Deaktivieren Sie: "Importierte Version als aktuelle Version festlegen"

  Hinweis: Diese Optionen sind ideal, wenn der Import Operatoren einschließt, deren Zielhosts noch nicht mit ihrem Kontaktpunktnamen in der Importumgebung definiert sind. Mit dieser Einstellung können Sie Objekte als aktuell festlegen, nachdem Sie sichergestellt haben, dass die Prozessziele in der Importumgebung verfügbar sind.

- Um den Import eines Objekts mit dupliziertem Namen aufzuschieben und das Objekt manuell als aktuell festlegen:
  - Aktivieren Sie: Nicht importieren
  - Deaktivieren Sie: "Importierte Version als aktuelle Version festlegen"
  - **Hinweis:** Diese Optionen sind ideal, wenn Sie neue Objekte in einen aufgefüllten Ordner importieren. Diese Optionen vermeiden, dass ein Importobjekt als neue Version eines Objekts mit demselben Namen und einer abweichenden Funktion festgelegt wird. Mit diesen Optionen können Sie Objekte auch als aktuell festlegen, nachdem Sie ihre Verwendung in der neuen Umgebung getestet und verifiziert haben.

    Wenn Sie Alarmmeldungen bekommen, erwägen Sie die folgenden Aktionen:

    - Zeichnen Sie die duplizierten Namen, in der Warnmeldung erscheinen, auf, und informieren Sie einen Administrator in der Quellumgebung. Vielleicht können diese Objekte umbenannt und erneut exportiert werden.
    - Importieren Sie sie erneut, jedoch in einen leeren Ordner.

- Um die importierten Objekte zu aktivieren, ohne die Aktion für Objekte mit duplizierten Namen zurückzusetzen:
  - Aktivieren Sie: Importieren und ersetzen
  - Aktivieren Sie: Importierte Version als aktuelle Version festlegen
  - **Hinweis:** Diese Optionen sind ideal, wenn Sie Objekte mit Fixes erneut in den Zielordner importieren. In diesem Fall müssen Sie niemals zur ersetzten Version zurückkehren.

Importieren eines Pakets mit vordefiniertem Inhalt

Administratoren wählen den Koordinationsrechner und anschließend den Zielordner aus und rufen den Importvorgang auf. Wenn das Importergebnis ein Paket mit vordefiniertem Inhalt ist, enthält es eine Reihe von Baseline-Objekten für das gleiche Release. Sie können die Werte für die Release-Versionen von Objekten in einem importierten Paket mit vordefiniertem Inhalt nicht ändern.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Bibliothek.
2. Klicken Sie auf Koordinationsrechner, und wählen Sie die Koordinationsrechner-*Zielumgebung* aus.

3. Klicken Sie mit der rechten Maustaste auf den Zielordner, und wählen Sie Importieren aus.

4. Klicken Sie auf Durchsuchen, und navigieren Sie zum Speicherort der exportierten Datei auf Ihrem lokalen Laufwerk. Wählen Sie die exportierte XML-Datei aus, und klicken Sie auf Öffnen.

5. Wählen Sie aus, wie ein Objekt importiert werden soll, das denselben Namen wie ein vorhandenes Objekt im gleichen Pfad hat.

   - Wählen Sie Importieren aus, um alle Objekte jeweils als eine neue Version des vorhandenen Objekts zu importieren.

     Diese Option eignet sich für Upgrades, wenn Sie den Verlauf von Vorgängerversionen beibehalten wollen.

     Hinweis: Wenn ein vorhandenes Objekt die gleiche Release-Version wie das importierte Objekt hat, ersetzt das importierte Objekt die duplizierte Version.

   - Wählen Sie Nicht importieren aus, um den Import des Objekts anzuhalten und das vorhandene Objekt beizubehalten.

     Wenn Sie diese Option auswählen, listet der Importprozess die Objekte mit Konflikt verursachenden Namen auf. Wenn Konflikte auftreten, können Sie den Importvorgang erneut durchführen und in einen leeren Ordner importieren. Alternativ können Sie das Objekt in der Quellumgebung umbenennen und dann den Export und Import wiederholen. Diese Option ist eine gute Wahl, wenn die zu importierenden Objekte neue Objekte sind und keine neuen Versionen von vorhandenen Objekten.

   – Wählen Sie Importieren und ersetzen aus, um das vorhandene Objekt zu löschen und die neue Version des Objekts als Version 0 zu importieren.

6. Wählen Sie aus, ob die Version der Objekte im Importordner als aktuelle Version festgelegt werden soll.

   - Wählen Sie Importierte Version als aktuelle Version festlegen aus, um die importierte Version sofort nach dem Import zu aktivieren. Wenn das importierte Objekt ein Upgrade ist, verwenden vorhandene Prozesse, die Vorgängerversionen von Objekten verwendet haben, nun die importierte Version. Die importierten Objekte können einen Prozess mit den Operatorzielen, die in der Importumgebung konfiguriert sind, einschließen. In diesem Fall können Sie den aktualisierten Prozess überprüfen, ohne Versionen zurückzusetzen.

   - Deaktivieren Sie Importierte Version als aktuelle Version festlegen, um das Festlegen als "Aktuell" später manuell durchzuführen. Deaktivieren Sie diese Option zum Beispiel, wenn der Import einen Prozess enthält, in dem die Ziele der Operatoren in dieser Umgebung noch nicht definiert sind.

7. Wählen Sie aus, ob importierte anwenderspezifische Operatoren zur Verfügung gestellt werden sollen.
   - Aktivieren Sie Importierte anwenderspezifische Operatoren verfügbar machen, um die Einstellung zu automatisieren, damit alle importierten anwenderspezifischen Operatoren verfügbar gemacht werden.
   - Deaktivieren Sie Importierte anwenderspezifische Operatoren verfügbar machen, um importierte anwenderspezifische Operatoren in einem nicht verfügbaren Status beizubehalten und sie einzeln manuell verfügbar zu machen.
8. Wählen Sie aus, ob Sie eine anwenderspezifische Operatorgruppe auf der Registerkarte "Module" veröffentlichen.
   - Aktivieren Sie Konfiguration der anwenderspezifischen Operatorgruppe veröffentlichen, wenn der Import neue anwenderspezifische Operatoren und eine neue anwenderspezifische Operatorgruppe einschließt und Sie in eine Domäne importieren, die von der Export-Domäne abweicht.
   - Deaktivieren Sie Konfiguration der anwenderspezifischen Operatorgruppe veröffentlichen in den folgenden Fällen:
     - Die Importumgebung befindet sich in derselben Domäne wie die Exportumgebung.
     - Die importierten anwenderspezifischen Operatoren sind neue Versionen von vorhandenen anwenderspezifischen Operatoren. In diesem Fall sind die anwenderspezifischen Operatorgruppen vorhanden.
     - Sie ziehen vor, dass ein Administrator neue Konfigurationen für anwenderspezifische Operatorgruppen manuell veröffentlicht.
9. Klicken Sie auf Senden, um den Importprozess zu starten.
10. Klicken Sie in der Meldung zur Verifizierung eines erfolgreichen Imports auf OK.

    Das Paket wird erfolgreich in den ausgewählten Ordner importiert. Das Paket wird auch im Auswahlmenü "Vordefinierte Inhalte" in der Registerkarte "Vorgänge" angezeigt. Wenn Sie ein Paket mit vordefinierten Inhalten aus dem Auswahlmenü auswählen, werden die Eigenschaften angezeigt. Die angezeigte Eigenschaft ist der Wert für die Release-Version, der für den Ordner festgelegt wurde, bevor es als vordefinierter Inhalt exportiert wurde.

Beispiel: Exportieren und Importieren von vordefinierten Inhalten

Exportieren Sie ein Paket aus der Bibliothek in der Quellumgebung (Designumgebung) als vordefinierter Inhalt, und speichern Sie die resultierende XML-Datei. Importieren Sie ein Paket mit vordefiniertem Inhalt in die Bibliothek der Zielumgebung (Produktionsumgebung), indem Sie nach der XML-Datei suchen und Importoptionen angeben.

Exportieren als vordefinierter Inhalt

1. Klicken Sie auf die Registerkarte Bibliothek für die *Koordinationsrechner-Umgebung*, die den Ordner mit den Objekten für die Übertragung enthält.
2. Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie Als vordefinierten Inhalt exportieren, Relative Pfade aus.

   Diese Auswahl kopiert das Paket in einen anderen Ordner als den Stammordner.

Equation 1: Die Rechtsklick-Optionen für Ordner umfassen "Exportieren" und "Als vordefinierten Inhalt exportieren". Bei beiden Exportoptionen kann "Absolute Pfade" oder "Relative Pfade" ausgewählt werden.



3. Speichern Sie die Datei in einem Ordner auf Ihrem lokalen Laufwerk oder auf einem Laufwerk, das Sie zugeordnet haben.
4. Klicken Sie auf Ordner öffnen. Der Ordner, in dem Sie die XML-Datei des Exports gespeichert haben, wird geöffnet, wenn der Download abgeschlossen ist.

Importieren eines Pakets mit vordefiniertem Inhalt

1. Klicken Sie auf die Registerkarte Bibliothek, und wählen Sie die *Koordinationsrechner-Umgebung* aus, die das Ziel für den Export- und Importprozess ist.
2. Navigieren Sie zum Ordner, in den die XML-Datei importiert werden soll, klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie Importieren aus.

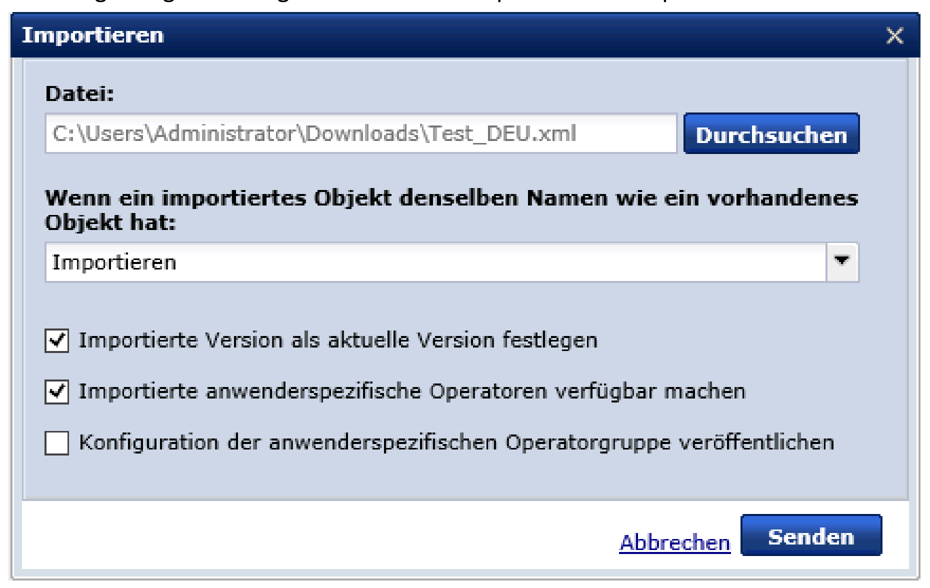
3. Klicken Sie auf Durchsuchen, navigieren Sie zum Speicherort, zu dem Sie die Datei exportiert haben, und klicken Sie auf Öffnen.

   Aktivieren Sie in diesem Beispiel die folgenden Optionen:

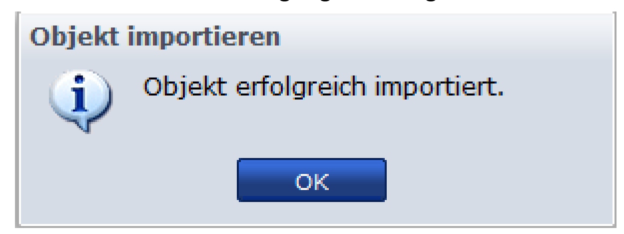
   - Importieren
   - Importierte Version als aktuelle Version festlegen
   - Importierte anwenderspezifische Operatoren verfügbar machen

     Hinweis: Wenn Sie diese Option nicht auswählen, werden anwenderspezifische Operatoren in CA Process Automation als nicht verfügbar importiert.

     Hinweis: Wählen Sie Konfiguration der anwenderspezifischen Operatorgruppe veröffentlichen nicht aus, wenn das Importpaket einen oder mehrere anwenderspezifische Operatoren enthält, für die eine neue anwenderspezifische Operatorgruppe in der Domäne veröffentlicht wurde, zu der die Importumgebung gehört. Die veröffentlichte Gruppe ist bereits in der Registerkarte "Module" im Konfigurationsbrowser vorhanden, wenn zwischen Umgebungen in der gleichen Domäne exportiert und importiert wird.



4. Klicken Sie auf Senden.
5. Klicken Sie in der Bestätigungsmeldung auf OK.



Der importierte vordefinierte Inhalt wird in dem von Ihnen ausgewählten Importordner angezeigt. Sie können vordefinierten Inhalt auch im Auswahlmenü "Vordefinierte Inhalte" auf der Registerkarte "Vorgänge" finden. Wenn Sie auf den vordefinierten Inhalt im linken Bereich klicken, werden seine Eigenschaften im rechten Bereich angezeigt.

6. Wählen Sie im Importordner das importierte Paket aus, und klicken Sie auf Eigenschaften.

7. Klicken Sie auf die Registerkarte Release.

   Die Daten für die Release-Version des vordefinierten Inhalts sind die gleichen wie beim Export. Wenn Sie mit der Maus auf das Feld Release-Version zeigen, weist die QuickInfo darauf hin, dass Sie den Wert für die Release-Version des Pakets nicht ändern können.

8. Wenn Sie auf den vordefinierten Inhalt doppelklicken, werden Sie das Folgende bemerken:

   - Alle importierten Objekte werden im gleichen Zielordner angezeigt.
   - Aus allen importierten Objekten wird eine Baseline erstellt.
   - Alle importierten Objekte enthalten den Text der Release-Version, der vor dem Export für das Objekt festgelegt wurde.

Überprüfen, dass der Prozess einwandfrei funktioniert

Bevor der Inhalt eines importierten Pakets für die Produktionsverwendung freigegeben wird, führt der Administrator den Prozess aus und überwacht die Ergebnisse. Ein erfolgreicher Ablauf impliziert, dass der Import des vordefinierten Inhalts alle erforderlichen Objektkomponenten enthalten hat, und dass alle Ziele richtig konfiguriert sind.

Der Verifizierungsschritt kann eine Überprüfung beinhalten, um sicherzustellen, dass der automatisierte Startmechanismus funktioniert, unabhängig davon, ob es sich um einen Ablaufplan, Formulare oder Auslöser handelt. Aktivieren Sie bei Bedarf Auslöser.

In seiner einfachsten Form kann der Verifizierungsprozess folgendermaßen zusammengefasst werden.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte Bibliothek, und wählen Sie die **Koordinationsrechner**-*Umgebung* des Importziels aus.
2. Klicken Sie auf die Registerkarte Vorgänge.
3. Starten Sie den Prozess durch den geplanten Startmechanismus.
4. Überwachen Sie den laufenden Prozess, bis er abgeschlossen wird. Antworten Sie auf alle Formulare, sodass der Prozess fortgesetzt werden kann.

5. Wenn der Prozess nicht erfolgreich ausgeführt wird, geben Sie ihn zur Fehlerbehebung an den Inhaltsdesigner zurück.
6. Wenn der Prozess Verzweigungen enthält, erstellen Sie für jede einen Testfall. Starten Sie anschließend den Prozess, und überwachen Sie ihn.
7. Führen Sie eine der folgenden Aktionen aus:
   - Wenn der Prozess nicht erfolgreich ausgeführt wird, geben Sie ihn zur Fehlerbehebung an den Inhaltsdesigner zurück.
   - Läuft der Prozess erfolgreich, übergeben Sie ihn an den Produktionsadministrator.
8. Wenn Sie ein Objekt identifizieren, das zusätzlichen Designaufwand benötigt, verwenden Sie den folgenden Prozess:
   a. Ein Inhaltsdesigner behebt das Problem und führt einen Test aus, um zu verifizieren, ob es korrekt behoben wurde.
   b. Inhaltsdesigner bereiten einen neuen Ordner für das Exportieren als vordefinierter Inhalt vor. Dafür muss eine neue Release-Version für den Ordner und alle Objekte, aus denen das Release besteht, festgelegt werden. Weitere Informationen finden Sie in Szenario: Vorbereiten eines Ordners für das Exportieren als vordefinierter Inhalt.
   c. Exportieren und importieren Sie diesen Ordner erneut als vordefinierter Inhalt. Weitere Informationen finden Sie in Szenario: Exportieren und Importieren von Objekten in einem Paket mit vordefiniertem Inhalt (siehe Seite 390).
   d. Überprüfen Sie erneut, ob der Prozess einwandfrei funktioniert.

Weitere Informationen:

Vorbereiten der Produktionsumgebung für eine neue Version (siehe Seite 388)

Verwenden des Papierkorbs

Der Papierkorb enthält Ordner und Objekte, die Sie und andere Anwender aus der Bibliothek gelöscht haben.

Durch die *Bereinigungsaktion* werden die ausgewählten Objekte oder Ordner dauerhaft aus der Bibliothek gelöscht.

Mit der *Wiederherstellungsaktion* werden die ausgewählten Objekte oder Ordner wiederhergestellt. Bei der Wiederherstellung werden auch zuvor gelöschte Ordner unter dem Pfad von wiederhergestellten Objekten berücksichtigt.

Wählen Sie die Aktion aus, die Sie ausführen möchten, um Details anzuzeigen:

- Durchsuchen des Papierkorbs (siehe Seite 406)
- Wiederherstellen von Objekten und Ordnern (siehe Seite 408)
- Bereinigen von Objekten und Ordnern (siehe Seite 409)

Durchsuchen des Papierkorbs

Sie können den Papierkorb mit einer Basissuche oder einer erweiterten Suche durchsuchen. Mit einer Basissuche wird nach dem Namen gefiltert, wenn die Eingabe der ganze Name oder eine Zeichenfolge ist, mit der einige Namen beginnen. Die erweiterte Suche bietet viele Suchkriterien.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek", minimieren Sie den Stammordner, und wählen Sie den Papierkorb aus.

   Alle gegenwärtig gelöschten Automatisierungsobjekte und Ordner werden im Hauptfenster angezeigt.

2. Geben Sie eine von einem Sternchen (*) gefolgte Zeichenfolge in das Suchfeld ein, und klicken Sie auf "Suchen", um eine einfache Suche auszuführen. Geben Sie zum Beispiel "Custom*" ein, um die Anzeige auf Objekte zu beschränken, deren Namen mit der Zeichenfolge "Custom" anfangen.

   Ordner und Automatisierungsobjekte mit Namen, die mit Ihrer Eingabe übereinstimmen, werden in der gefilterten Liste angezeigt.

3. Klicken Sie auf "Erweiterte Suche", um Attribute anzuzeigen, mit denen die Suche durchgeführt wird. Sie können einen oder mehr Arten von Suchkriterien eingeben.

   - Schlüsselwörter – Geben Sie einzelne oder mehrere Schlüsselwörter ein, um Objekte oder Ordner zu suchen, denen die angegebenen Schlüsselwörter zugewiesen wurden. Wenn Sie mehr als ein Schlüsselwort angeben, verwenden Sie als Trennzeichen ein Komma (,).

     - Um nach Objekten zu filtern, die durch eines der von Ihnen angegebenen Schlüsselwörter definiert wurden, wählen Sie das standardmäßig ausgewählte ODER aus.

     - Um nach Objekten zu filtern, die mit allen von Ihnen angegebenen Schlüsselwörtern definiert wurden, wählen Sie UND aus.

   - Name – Name des Ordners oder Automatisierungsobjekts.

   - Verantwortliche - Anwender-ID des Objekt- oder Ordnerverantwortlichen. Der Standardeigentümer ist der Anwender, der das Objekt erstellte. Ein neuer Verantwortlicher kann mit "Verantwortlichen festlegen" angegeben werden.

   - Typ – Wählen Sie einen Automatisierungsobjekttyp aus der Drop-down-Liste aus.

   - Zustand – Wählen Sie einen Zustand aus der Drop-down-Liste aus.

   - Änderungsdatum – Verwenden Sie die Kalender, um den Datumsbereich auszuwählen, in dem die Elemente, die Sie anzeigen möchten, geändert wurden.

   - Erstellungsdatum – Verwenden Sie die Kalender, um den Datumsbereich auszuwählen, in dem die Elemente, die Sie anzeigen möchten, erstellt wurden.

4. Klicken Sie auf "Suche".
5. Führen Sie die Bereinigungs- oder Wiederherstellungsaktion für den Ergebnissatz aus.
6. Klicken Sie auf "Zurücksetzen", um die Suchkriterien zu löschen, wenn Sie direkt eine andere Suche durchführen möchten.

Wiederherstellen von Objekten und Ordnern

Wenn Sie ein Objekt oder einen Ordner aus der Bibliothek löschen, wird es bzw. er in den Papierkorb verschoben. Vom Papierkorb aus können Sie ein Objekt oder einen Ordner wiederherstellen, das bzw. den Sie gelöscht haben. Über die Wiederherstellung werden das Objekt oder der Ordner und andere Ordner im gelöschten Pfad wiederhergestellt. Sie können angeben, ob Objekte im Zielpfad, die den gleichen Namen wie ausgewählte Objekte aufweisen, überschrieben werden sollen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek", blenden Sie den Stammordner im linken Bereich aus, und wählen Sie Papierkorb aus.

   Das Hauptraster wird aktualisiert, und alle Automatisierungsobjekte und Ordner werden angezeigt, die sich gegenwärtig im Papierkorb befinden.

2. Wählen Sie ein oder mehrere Objekte oder Ordner aus, und klicken Sie auf Auswahl wiederherstellen.

3. Klicken Sie in der Bestätigungsmeldung auf Ja, um die Wiederherstellung durchzuführen.

   - Wenn im Zielpfad kein Objekt mit dem gleichen Namen wie ein ausgewähltes Objekt vorhanden ist, stellt die Anwendung das ausgewählte Objekt am Zielspeicherort wieder her.

   - Wenn im Zielpfad ein Objekt mit dem gleichen Namen wie ein wiederherzustellendes Objekt vorhanden ist, wird eine Warnung angezeigt. Führen Sie eine der folgenden Aktionen aus:

     - Wählen Sie das Objekt aus, und klicken Sie auf OK, um mit der Wiederherstellung fortzufahren.

       Die Anwendung verschiebt das Objekt vom Papierkorb in den Zielpfad und überschreibt das Objekt, das im Zielpfad vorhanden ist.

     - Klicken Sie auf Abbrechen, um die Wiederherstellung für das Objekt anzuhalten.

       Das Objekt im Zielpfad wird von der Anwendung nicht überschrieben. Erwägen Sie in diesem Fall, das Objekt mit dem duplizierten Namen zu verschieben oder umzubenennen, und versuchen Sie den Wiederherstellungsvorgang erneut.

   Der Wiederherstellungsprozess stellt die ausgewählten Objekte und gegebenenfalls ihre Ordnerpfade wieder her.

Bereinigen von Objekten und Ordnern

Der Papierkorb ist als temporärer Container für gelöschte Objekte vorgesehen, sodass Inhaltsdesigner Objekte wiederherstellen können, die sie versehentlich gelöscht haben.

Die regelmäßige Bereinigung von veralteten Objekten führt zu einem aufgeräumten Papierkorb. Als Administrator können Sie ausgewählte Automatisierungsobjekte und Ordner bereinigen. Alternativ können Sie den Inhalt des Papierkorbs in einem einzigen Schritt bereinigen. Ein bereinigtes Objekt kann nicht abgerufen oder nicht wiederhergestellt werden.

Gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Registerkarte "Bibliothek".
2. Klicken Sie auf Koordinationsrechner, und wählen Sie die geeignete *Koordinationsrechner-Umgebung* aus.
3. Wenn der Papierkorb nicht sichtbar ist, minimieren Sie den Stammordner.
4. Klicken Sie auf den Papierkorb.

   Alle Automatisierungsobjekte und Ordner, die aus der Bibliothek gelöscht wurden, werden im Hauptbereichsraster angezeigt.
5. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie spezifische Objekte aus, und klicken Sie dann auf "Auswahl bereinigen".
   - Klicken Sie auf Alle bereinigen.
6. Wenn Sie die Bereinigung für ausgewählte Objekte initiierten, wird eine Bestätigungsmeldung angezeigt.
   - Klicken Sie auf "Nein", um die Bereinigung abzubrechen, stellen Sie die erforderlichen Objekte in der Bibliothek wieder her, starten Sie die Bereinigung neu.
   - Klicken Sie auf "Ja", um mit dem Bereinigungsprozess fortzufahren.
7. Wenn Sie eine Bereinigung aller Prozesse initiiert haben, wo die Inhalte des Papierkorbs ausgecheckte Objekte enthalten, wird ein Dialogfeld angezeigt, das diese Objekte auflistet. Werten Sie die Liste aus, und führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie auf "Nein", um die Bereinigung abzubrechen, stellen Sie die erforderlichen Objekte in der Bibliothek wieder her, starten Sie die Bereinigung neu.
   - Klicken Sie auf "Ja", um mit dem Bereinigungsprozess fortzufahren.

Anhang A: FIPS 140-2-Support

Die Veröffentlichung "Federal Information Processing Standard (FIPS) 140-2", *Security Requirements for Cryptographic Modules,* definiert eine Reihe von Anforderungen für Produkte, die vertrauliche Daten verschlüsseln. Der Standard stellt vier Sicherheitsebenen bereit, die einen weiten Bereich von potenziellen Anwendungen und Umgebungen abdecken sollen. Der Bereich "Security Management and Assurance (SMA)" von NIST validiert kryptografische Module und kryptografische Algorithmusimplementierungen. Bei einer Validierung veröffentlicht SMA den Lieferanten und die Zertifikatsnummer der Validierungen mit Modulnamen.

Wenn FIPS 140-2 unterstützt wird, verwendet CA Process Automation kryptografische Module aus den Bibliotheken von RSA BSAFE® Crypto-J. RSA ist die Security Division von EMC.

Dieses Kapitel enthält folgende Themen:

Wenn CA Process Automation Verschlüsselung verwendet

CA Process Automation verschlüsselt Kommunikation und verschlüsselt die Datenspeicher. CA Process Automation verwendet Module, die nach FIPS 140-2 validiert werden, die für die Sicherheit erforderlich sind.

Beispiel:

- Bei der Übertragung von Daten zwischen dem Koordinationsrechner und Agenten werden die Daten verschlüsselt.
- Bei der Übertragung von Daten zwischen dem Koordinationsrechner und dem CA Process Automation-Client werden vertrauliche Daten verschlüsselt.
- Bei der Übertragung von Daten zwischen CA EEM und CA Process Automation werden die Daten verschlüsselt. (Version 03.1.00 und später).
- Wenn ein System, das aus Automatisierungsobjekten besteht, mithilfe von Exportieren und Importieren übertragen wird, werden alle Kennwort-Objekte im System verschlüsselt.
- Wenn vertrauliche Daten, wie z. B. Kennwörter, in Dateisystemen gespeichert sind, werden diese Daten verschlüsselt.

Kryptografisches Module nach FIPS 140-2 validiert

CA Process Automation verwendet ein eingebettetes kryptografisches Modul, das mit diesen Spezifikationen nach FIPS 140-2 validiert ist:

- Cert#: 1048
- Lieferant: RSA, The Security Division of EMC
- Kryptografisches Modul: RSA BSAFE® Crypto-J JCE Provider Module (Software Version: 4.0)
- Modultyp: Software
- Validierungsdaten: 27.10.2008, 26.01.2009. 07.09.2010
- Ebene/Beschreibung: Allgemeine Ebene 1
- FIPS-genehmigter Algorithmus: RSA (Cert. #311)

Für weitere Informationen, verwenden Sie eine Suchmaschine und suchen Sie die Sicherheitsrichtlinie *RSA BSAFE Crypto-J JCE Provider Module*. Diese Richtlinie listet die Plattformen auf, auf denen die Algorithmen einschließlich Plattformen von Microsoft, Linux, Oracle (Solaris), HP und IBM kompatibel sind. Dieses Dokument enthält auf Details zu Crypto-J-FIPS-genehmigten Algorithmen.

Im Nur-FIPS-Modus verwendet CA EEM folgende Algorithmen:

- SHA1, SHA256, SHA384: Für die Verwaltung der Client-Server-Kommunikation.
- SHA512: Für das Speichern von Anwenderkennwörtern.

  Hinweis: CA EEM wendet SHA512 nur dann auf den Kennwort-Digest an, wenn Sie den Kennwort-Digest aktualisieren. Bis zur Aktualisierung akzeptiert CA EEM das vorhandene Kennwort im Kennwort-Digest.
- SHA256: Für die Verwaltung von Anwendungszertifikaten.
- TLS-v1.0: Für Kommunikation mit externen LDAP-Verzeichnissen, wenn die LDAP-Verbindung über TLS erfolgt.

Verwalten von IP-Adressen

Möglicherweise ist das Verwalten von IP-Adressen erforderlich. Einige Beispiele:

- Ändern der IP-Adresse und Namen eines Koordinationsrechners.

  Ändern Sie die Kombination der Namen und IP-Adresse, unabhängig davon, wo sie in folgenden Dateien angezeigt werden.

  Installationsverzeichnis/server/c2o/.config/OasisConfig.properties

  Installationsverzeichnis/server/c2o/.config/Domain.xml

  Hinweis: Um weiterhin einen unveränderten Hostnamen in allen Referenzen in CA Process Automation zu verwenden, ändern Sie das DNS mit der neuen IP-Adresse.

- Wenn Sie Agenten mithilfe von geänderten IP-Adressen installieren, konfigurieren Sie den Agenten neu, indem Sie folgende Datei aktualisieren:

  Installationsverzeichnis/PAM Agent/PAMAgent/.config/OasisConfig.properties

  Ändern Sie den Wert der folgenden Eigenschaft:

  oasis.jxta.host

- Verwenden Sie mehrere IP-Adressen für CA Process Automation, wenn Sie zwei NICs haben, eine interne und eine andere externe.

  Damit CA Process Automation an die externe IP-Adresse gebunden wird, fügen Sie der Datei "OasisConfig.properties" folgende Eigenschaft hinzu:

  jboss.bind.address=*xxx.xxx.xxx.xxx*

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Authentifizierung und Autorisierung von Anwendern im FIPS-Modus

CA EEM kann für die Verwendung im FIPS-Modus konfiguriert werden. Dies ist eine Option. Damit CA Process Automation für FIPS konfiguriert werden kann, muss CA EEM für die Verwendung im FIPS-Modus konfiguriert sein. CA Process Automation kann auch ohne FIPS verwendet werden, wenn CA EEM für die Verwendung im FIPS-Modus konfiguriert ist.

Daten, die zwischen CA EEM und CA Process Automation übertragen werden, werden unabhängig davon, ob der FIPS-Modus aktiviert ist, verschlüsselt. Der Unterschied sind die verwendeten Algorithmen für die Verschlüsselung.

Wenn Anwender sich anmelden, überträgt CA Process Automation den Anwendernamen und Kennwort auf CA EEM. CA EEM gibt CA Process Automation Authentifizierungs- und Autorisierungsdaten zurück.

- Wenn FIPS-Modus aktiviert ist:
  - Übertragene Daten werden mit dem SHA1-Algorithmus verschlüsselt, der von FIPS unterstützt wird.
  - Ein PAM.cer-Zertifikat wird verwendet.
- Wenn FIPS-Modus deaktiviert ist:
  - Übertragene Daten werden mit dem MD5-Algorithmus verschlüsselt.
  - Ein PAM.p12-Zertifikat wird verwendet.

Anhang B: Verwalten der Domäne

Das Verwalten der Domäne beinhaltet einige Aufgaben, die Sie außerhalb der Registerkarte "Konfiguration" ausführen.

Dieses Kapitel enthält folgende Themen:

Einrichten der Domäne

Für das Einrichten eines System sind sowohl physische als auch logische Änderungen erforderlich. Das physische System wird durch die Installation eingerichtet. Sie richten Ihr logisches System innerhalb CA Process Automation ein.

- Wenn zusätzliche Kapazitäten in der Designumgebung benötigt werden, fügen Sie dem Domänen-Koordinationsrechner einen Knoten hinzu.
- Wenn zusätzliche Kapazitäten in der Produktionsumgebung benötigt werden, fügen Sie dem Domänen-Koordinationsrechner einen Knoten hinzu. Fügen Sie einen Software- oder Hardware-Lastenausgleich hinzu.

  Hinweis: Weitere Informationen hierzu finden Sie im *Installationshandbuch.*
- Wenn ein Server, auf dem ein Koordinationsrechner installiert ist, außer Betrieb übernommen wird, exportieren Sie den Stammknoten der Bibliothek und importieren Sie ihn in einen neuen Koordinationsrechner.
- Wenn neue Anwender benötigt oder neue Rollen hinzugefügt werden, aktualisieren Sie CA EEM mit Änderungen an Anwenderkonten und Richtlinien.

Sichern der Domäne

Führen Sie eine Sicherung von CA Process Automation mit dem Sicherungs-Tool durch, das Sie auf Ihrer Site verwenden.

Gehen Sie folgendermaßen vor:

1. Sichern Sie jedes Vorkommen der folgenden drei CA Process Automation-Datenbanken:
   - Repository
   - Runtime
   - Berichterstellung
2. Sichern Sie das folgende Verzeichnis:

   `Installationsverzeichnis/server/c2o/.config`
3. Sichern Sie die Bibliotheksinhalte, indem Sie den Stammordner in der Registerkarte "Bibliothek" exportieren.

Wiederherstellen der Domäne aus den Sicherungen

CA Process Automation kann aufgrund von Datenbeschädigung, Fehlkonfiguration oder Speicherverlust auf einem geclusterten Domänen-Koordinationsrechner fehlschlagen. Sie können nach so einem Fehler eine Datenwiederherstellung durchführen und die Daten in CA Process Automation wiederherstellen.

Sie können Ihre Verwendung von CA Process Automation nach einem Fehler wiederherstellen. Die Vorgehensweise ist das Ausführen einer neuen Installation des Domänen-Koordinationsrechners, den Sie herunterfahren, sobald er installiert ist. Sie ersetzen die leeren Datenbanken durch Ihre Datenbanksicherungen und stellen Ihre Konfigurationsdatei aus einem Backup wieder her. Dann starten Sie CA Process Automation und überprüfen, ob die wiederhergestellten Daten vorhanden sind.

Gehen Sie folgendermaßen vor:

1. Bereiten Sie die Installation vor. Richten Sie sich nach dem *Installationshandbuch,* nachdem Sie folgende Vorbereitungen abgeschlossen haben:
   - Überprüfen Sie, ob die Hardware, das Betriebssystem und das Datenbankmodul installiert sind.
   - Überprüfen Sie, ob die erforderlichen Drittanbieterkomponenten installiert sind.
   - Installieren und Konfigurieren von CA EEM.
2. Führen Sie eine neue Installation von CA Process Automation aus, wie im *Installationshandbuch* beschrieben.
3. Fügen Sie nach Bedarf Knoten hinzu, um den ursprünglichen Cluster darzustellen. Weitere Informationen hierzu finden Sie im *Installationshandbuch*.
4. Halten Sie CA Process Automation an.
5. Stellen Sie Ihr System aus den Sicherungen wieder her.
   a. Ersetzen Sie die Repository-Datenbank, Laufzeitdatenbank und Berichtsdatenbank durch ihre jeweiligen Datenbanksicherungen.
   b. Benennen Sie den aktuellen Ordner ".config" in:

      Installationsverzeichnis/server/c2o/.config
   c. Stellen Sie Folgendes aus der Sicherung wieder her:

      Installationsverzeichnis/server/c2o/.config
6. Starten Sie CA Process Automation.
7. Überprüfen Sie, ob Ihre Konfiguration wiederhergestellt wurde.
8. Überprüfen Sie, ob Ihre Datenbankdaten intakt sind.

Verwalten von Zertifikaten

Zum Verwalten von Zertifikaten gehören folgende Vorgänge:

- Installieren des vordefinierten CA Process Automation-Zertifikats (siehe Seite 420).
- Erstellen und Implementieren von eigenen Zertifikaten für CA Process Automation (siehe Seite 422).
- Implementieren Ihres Vertrauenswürdigen SSL-Zertifikats eines Drittanbieters für CA Process Automation (siehe Seite 425).

Kennwortschutz durch CA Process Automation

Anwenderkonto-Anmeldeinformationen, also Anwendername und Kennwort, werden verwendet, um Zugriff auf verschiedene Systeme und Funktionen zu erhalten. Der Kennwortwert muss aus Sicherheitsgründen geschützt werden. Obwohl Kennwörter Zeichenfolgen sind, werden sie anders als andere Werte dieses Datentyps behandelt. CA Process Automation schützt Kennwörter auf der Anwenderoberflächenebene auf folgende Weisen:

- Anwender können Kennwörter nicht von Ort zu Ort weitergeben.
- Anwender können keinen CA Process Automation-Prozess schreiben, der "process.v = process.Password" festlegt, weil v sichtbar ist.
- Manipulationen, wie ein Kennwort durch den Buchstaben "t" zu ergänzen und dann später das "t" zu entfernen, werden mithilfe von JavaScripts deaktiviert.
- Anwender können keine Kennwörter mit einem +-Operator verketten. Alle Aktionen, die den Kennwortwert enthüllen würden, sind unzulässig.
- Anwender können die Erkennung von Kennwortinhalten nicht aktivieren. Sie können zum Beispiel keine verstecken Inhalte sichtbar machen.

Unterm Strich sorgt CA Process Automation dafür, dass die Kennwortsicherheit garantiert wird, so lange sich das Kennwort innerhalb von CA Process Automation befindet. Kennwörter, die Teil der Konfiguration der Operatorkategorie sind, werden geschützt. Sie können nicht geändert, referenziert oder an externe Methoden weitergegeben werden.

Wenn ein Kennwort, das kein Teil der Konfiguration der Operatorkategorie ist, an eine externe Methode übergeben wird, kann es als Klartext zurückgegeben werden. Treffen Sie Vorkehrungen, um Kennwörter, die an externe Programme weitergegeben werden, zu schützen. Die beste Lösung besteht darin, Zertifikate oder eine Alternative zu verwenden.

Sie können die Inhalte der Definitionen, die in einer Datenbank gespeichert sind, exportieren und anschließend in eine Datenbank innerhalb der gleichen Domäne oder in eine andere Domäne importieren. Beim Importieren von Datensätzen in eine andere Domäne werden Kennwörter ausgeblendet, da Kennwörter verschlüsselt werden. Andere Domänen verwenden grundsätzliche andere Verschlüsselungscodes.

Informationen zum CA Process Automation-Zertifikat

Untersuchen Sie die Unterschiede zwischen dem Verwenden eines selbst unterzeichneten Zertifikats und eines Vertrauenswürdigen SSL-Zertifikats hinsichtlich Ihres Sicherheitsbedarfs für CA Process Automation.

CA Process Automation stellt ein selbst unterzeichnetes Zertifikat bereit, das für die Verwendung vorkonfiguriert ist. Sie können das CA Process Automation-Zertifikat in einer der folgenden Weisen verwalten:

- Verwenden Sie das mit CA Process Automation bereitgestellte Zertifikat. Installieren Sie dieses Zertifikat auf jedem Browser, von dem Sie auf die URL zum CA Process Automation-Domänen-Koordinationsrechner zugreifen.
- Erstellen Sie Ihr eigenes selbst unterzeichnetes Zertifikat mit einem bereitgestellten Hilfsprogramm, verschlüsseln Sie das Kennwort mit einem bereitgestellten Hilfsprogramm, aktualisieren Sie die Eigenschaftsdatei mit dem Schlüsselspeicher-Speicherort, dem verschlüsseltem Kennwort und dem Schlüsselspeicher-Alias.
- Erhalten Sie ein Zertifikat von einer anerkannten Zertifizierungsstelle. Aktualisieren Sie die Eigenschaftsdatei mit dem Schlüsselspeicher-Speicherort, dem verschlüsselten Kennwort und dem Schlüsselspeicher-Alias.

Wichtig! Entfernen Sie nicht den Standardschlüsselspeicher oder das selbst unterzeichnete Zertifikat, das mit CA Process Automation bereitgestellt wird. Dieses Zertifikat wird auch dann benötigt, wenn Sie CA Process Automation konfigurieren, um Ihr eigenes selbst unterzeichnetes Zertifikat oder eines zu verwenden, das Sie von einer Zertifizierungsstelle erhalten.

Installieren des vordefinierten CA Process Automation-Zertifikats

Wenn Sie auf CA Process Automation mit einer URL zugreifen, die das HTTPS-Protokoll verwendet, sucht der Browser nach einem von einer Zertifizierungsstelle herausgegebenen Zertifikat. Wenn Sie das selbst unterzeichnete CA Technologies-Zertifikat verwenden, wenn Sie CA Process Automation starten, zeigt der Browser eine Warnung an, dass das Zertifikat nicht vertrauenswürdig ist.

So installieren Sie das vordefinierte Zertifikat für CA Process Automation:

1. Öffnen Sie einen Browser, geben Sie die URL für CA Process Automation ein, und melden Sie sich an.
2. Wenn ein Sicherheitsalarm angezeigt wird, klicken Sie auf "Zertifikat anzeigen".
3. Klicken Sie auf "Zertifikat installieren", und klicken Sie auf "OK".
4. Schließen Sie den Assistenten ab.

   Bei Ihrer nächsten Anmeldung wird kein Sicherheitsalarm angezeigt.

Informationen zum Erstellen von selbstsignierten Zertifikaten

Sie können das selbstsignierte Zertifikat, das mit CA Process Automation mitgeliefert wird, ersetzen. Das vordefinierte Zertifikat wird in der OasisConfig.properties-Datei konfiguriert. Wenn Sie Ihr eigenes selbstsigniertes Zertifikat erstellen, aktualisieren Sie diese Eigenschaftsdatei, und führen Sie eine Batch-Datei aus, um die jar-Dateien (oder Java ARchive) zu signieren.

Bevor Sie Ihr eigenes Zertifikat erstellen, planen Sie Werte für den Schlüsselspeicher-Pfad und das Schlüsselspeicher-Alias. Sie geben diese Werte ein, wenn Sie Keytool ausführen und die Eigenschaftsdatei aktualisieren.

Sie verwenden die folgenden Dateien und Hilfsprogramme, um Ihre eigenen selbstsignierten Zertifikate zu implementieren:

- Hilfsprogramm "Keytool"

  Hinweis: Für Informationen zu diesem Java Sun-Hilfsprogramm suchen Sie nach Keytool - Schlüssel und Zertifikatsmanagement-Tool.

- PasswordEncryption.bat
- SignC2OJars.bat
- OasisConfig.properties-Datei, vor allem die folgenden drei Parameter
  - itpam.web.keystorepath=

    Standard:

    Installationsverzeichnis/server/c2o/.config/c2okeystore

    Hinweis: Der Standardwert ist der selbstsignierte Schlüsselspeicher-Pfad,

  - itpam.web.keystore.password=

    Der Standardwert verweist auf eine verschlüsselte Domänen-ID. (Führen Sie die PasswordEncryption.bat-Datei aus, und geben Sie das Schlüsselspeicher-Kennwort ein. Das Batch-Programm generiert das verschlüsselte Kennwort auf der Konsole, das Sie hier als neuen Wert angeben.)

  - itpam.web.keystorealias=

    Standard: ITPAM

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Erstellen und implementieren eines eigenen selbstsignierten Zertifikats

Sie können Ihr eigenes selbstsigniertes Zertifikat erstellen, um das selbstsignierte Zertifikat durch das mit CA Process Automation bereitgestellte zu ersetzen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich mit Administratoren-Anmeldeinformationen am Host an, auf dem der Ziel-Koordinationsrechner installiert ist.
2. Stoppen Sie den Koordinationsrechner (siehe Seite 206).
3. Wenn Sie den aktuellen Aliasnamen für den Schlüsselspeicher erneut verwenden möchten, entfernen Sie das Alias, bevor Sie fortfahren.
4. Führen Sie den folgenden Befehl aus, um einen Schlüsselspeicher mit dem Java-Tool, Keytool, zu erstellen. Geben Sie Ihre eigenen Werte für "aliasname" und für "keystore_name" an. Der Standardwert für "aliasname" ist "ITPAM". Wenn Sie keinen Pfad für Schlüsselspeicher eingeben, wird der aktuelle Pfad verwendet.

   ```
   keytool -genkey -alias "aliasname" -keyalg RSA -keystore
   "keystore_path.keystore"
   ```

   Akzeptieren Sie zum Beispiel den standardmäßigen Schlüsselspeicherpfad und geben Sie Folgendes ein:

   ```
   keytool -genkey -alias "PAM" -keyalg RSA
   ```

   Es werden Aufforderungen zur Eingabe und Bestätigung eines Schlüsselspeicher-Kennworts angezeigt.

5. Geben Sie das gleiche Schlüsselspeicher-Kennwort als Reaktion auf beide Aufforderungen ein. (Merken Sie sich dieses Kennwort für die spätere Eingabe in ein Verschlüsselungshilfsprogramm.)

   Eine Reihe von Aufforderungen wird gefolgt von einer Bestätigungsaufforderung angezeigt.

6. Reagieren Sie mit den angeforderten Distinguished Name-Informationen folgendermaßen auf Aufforderungen:

   a. Geben Sie Ihren Vor- und Nachnamen ein.

   b. Geben Sie den Namen Ihrer Organisationseinheit ein.

   c. Geben Sie den Namen Ihrer Organisation ein.

   d. Geben Sie den Namen Ihrer Stadt oder Region ein.

   e. Geben Sie den Namen Ihres Bundeslands oder Kantons ein.

   f. Geben Sie den zweistelligen Ländercode für Ihre Organisationseinheit ein.

   Eine Bestätigung Ihrer Eingaben wird im folgenden Format angezeigt: Ist CN=Wert, OU=Wert, O=Wert, L=Wert, ST=Wert, C=Wert korrekt?

7. Überprüfen Sie die Eingaben, und geben Sie zur Bestätigung "Ja" ein. (Geben Sie anderenfalls "Nein" ein, und reagieren Sie erneut auf die Aufforderungen.)
8. Reagieren Sie auf die Aufforderung zur Eingabe des Schlüsselkennworts für *aliasname* auf eine der folgenden Weisen. Bei der empfohlenen Option müssen Sie das Zertifikatskennwort nicht eingeben, da jedes Jar in Schritt 13 signiert wird.
   - Geben Sie ein eindeutiges Schlüsselkennwort für *aliasname* ein.
   - (Empfohlen) Drücken Sie die Eingabetaste, um das Schlüsselspeicher-Kennwort als Aliaskennwort zu benutzen.

   Ein neuer Schlüsselspeicher wird im aktuellen Verzeichnis erstellt.
9. (Optional) Verschieben Sie diesen Schlüsselspeicher in ein anderes Verzeichnis.
10. Verschlüsseln Sie das Schlüsselspeicher-Kennwort, das Sie in Schritt 5 eingegeben haben.
    a. Ändern Sie Verzeichnisse zum Verzeichnis "*Installationsverzeichnis*/server/c2o".
    b. Führen Sie PasswordEncryption.bat aus.
    c. Geben Sie das Schlüsselspeicher-Kennwort nach Aufforderung ein.

    Das Hilfsprogramm verschlüsselt das eingegebene Schlüsselspeicher-Kennwort und speichert die Ergebnisse in der Konsole.
11. Sichern Sie die OasisConfig.properties-Datei. (*Installationsverzeichnis*/server/c2o/.config/OasisConfig.properties)
12. Aktualisieren Sie die OasisConfiguration-Eigenschaftsdatei folgendermaßen:
    a. Geben Sie für "itpam.web.keystorepath=" den absoluten Pfad zum Schlüsselspeicher ein, wobei Sie anstelle von "\" den normalen Schrägstrich "/" verwenden, zum Beispiel C:/*Schlüsselspeicher-Pfad*/keystore.
    b. Kopieren Sie für "itpam.web.keystore.password=" das verschlüsselte Schlüsselspeicher-Kennwort, und fügen Sie es ein, das in Schritt 9 erstellt wurde.
    c. Geben Sie für "itpam.web.keystore.alias=" den im Keytool-Befehl in Schritt 4 angegebenen Aliasnamen ein.
13. Führen Sie "SignC2OJars.bat" aus, um die Jars zu signieren.

    Dieser Schritt ist erforderlich, nachdem das Zertifikat oder der Schlüsselspeicher aktualisiert wurde.
14. Starten Sie den Koordinationsrechner (siehe Seite 207).

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Informationen zum Verwenden eines von einer Zertifizierungsstelle eines Drittanbieters ausgestellten Zertifikats

CA Process Automation unterstützt Drittanbieter-Sicherheitszertifikate für den HTTPS-Webzugriff und das Signieren von JAR-Dateien. Verwenden Sie Ihre eigenen Ressourcen, um ein vertrauenswürdiges SSL-Zertifikat von der Zertifizierungsstelle Ihrer Wahl zu erhalten. Dieses Verfahren wird in diesem Handbuch nicht beschrieben.

Die Verwendung von Drittanbieter-Sicherheitszertifikaten erfordert die Verwendung von Drittanbieter-Tools. Der Einrichtungsprozess erfordert auch manuelle Änderungen der Eigenschaftsdatei "OasisConfig" (*Installationsverzeichnis*/server/c2o/.config/OasisConfig.properties). Bevor Sie beginnen, sollten Sie sich mit den grundlegenden Konzepten von Sicherheitszertifikaten und Schlüsselspeichern sowie mit dem Keytool-Hilfsprogramm, das mit dem Java JDK bereitgestellt wird, vertraut machen.

Das Implementieren von Drittanbieter-Sicherheitszertifikaten erfordert das Aktualisieren von Werten für drei Parameter in der Eigenschaftsdatei "OasisConfig":

- "itpam.web.keystorepath"

  Der Standardwert ist der Schlüsselspeicherpfad für das selbst unterzeichnete Zertifikat:

  `Installationsverzeichnis/server/c2o/.config/c2okeystore`

- "itpam.web.keystore.password"

  Der Standardwert ist die verschlüsselte "DOMAINID".

- "itpam.web.keystorealias"

  Der Standardwert ist "ITPAM".

  Hinweis: Ein Schlüsselspeicher kann mehr als ein Alias haben. Um einen Schlüsselspeicher-Alias zu verwenden, der einen vorhandenen Alias dupliziert, entfernen Sie den vorhandenen Alias, bevor Sie eine neue Instanz hinzuzufügen.

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Implementieren Ihres vertrauenswürdigen SSL-Zertifikats eines Drittanbieters

CA Process Automation unterstützt Drittanbieter-Sicherheitszertifikate für den HTTPS-Webzugriff und das Signieren von JAR-Dateien. Sie können solche Zertifikate von einer Drittanbieter-Zertifizierungsstelle erhalten.

Gehen Sie folgendermaßen vor:

1. Entscheiden Sie sich für ein Zertifikatskennwort, und rufen Sie ein Sicherheitszertifikat von einer Zertifizierungsstelle ab.
2. Importieren Sie unter Verwendung der Anweisungen der Zertifizierungsstelle das Zertifikat in einen Schlüsselspeicher.

   Normalerweise verwenden Sie einen Befehl wie keytool –import –alias *meinAlias* –file certfile –keystore "Pfad-_und_Dateiangaben_für_Schlüsselspeicher".
3. Geben Sie für das Schlüsselspeicherkennwort von der Zertifizierungsstelle bereitgestellte Zertifikatskennwort ein.
4. Rufen Sie eine verschlüsselte Version des Schlüsselspeicherkennworts ab.
   a. Navigieren Sie zu "*Installationsverzeichnis*\server\c2o".
   b. Suchen Sie das Kennwortverschlüsselungsskript ("PasswordEncryption.bat" für Windows, "PasswordEncryption.sh" für UNIX und Linux).
   c. Führen Sie "PasswordEncryption <zu_verschlüsselndes_Kennwort>" aus.
   d. Speichern Sie den langen verschlüsselten Wert, der für die Eingabe in der Eigenschaftsdatei zurückgegebenen wird.
5. Stoppen Sie den Koordinationsrechner (siehe Seite 206).
6. Sichern und bearbeiten Sie die Oasis-Konfigurationseigenschaftsdatei, um Folgendes hinzuzufügen oder zu aktualisieren:
   a. itpam.web.keystorepath zum Speicherort des Schlüsselspeichers mithilfe des vollqualifizierten Pfades und Dateinamens für die Schlüsselspeicherdatei.
   b. itpam.web.keystore.password mit dem verschlüsselten Schlüsselspeicher-Kennwort (setzen Sie verschlüsselte Kennwortwerte nicht in Anführungszeichen)
   c. itpam.web.keystorealias zu dem Alias, der verwendet wird, um auf das Zertifikat im Schlüsselspeicher zu verweisen ("meinAlias" in den Beispielen).

7. Signieren Sie JAR-Dateien, indem Sie "SignC2OJars" ("SignC2OJars.bat" für Windows, "SignC2OJars.sh" für UNIX und Linux) mit CA Process Automation in "*Installationsverzeichnis*\server\c2o" ausführen. Führen Sie "SignC2oJars" ohne Parameter aus, um die JAR-Dateien zu signieren. Wenn das eingegebene Schlüsselspeicherkennwort nicht mit dem Zertifikatskennwort übereinstimmt, geben Sie das Zertifikatskennwort bei jeder JAR-Signierung ein.

   Hinweis: Unter AIX besteht ein bekanntes Problem, wenn Sie eine JAR-Datei mithilfe von "SignC2OJars" erneut signieren. Um dieses Problem zu umgehen, müssen Sie die Signierung der JAR-Dateien manuell aufheben, indem Sie die *.SF- und *.RSA-Dateien im Ordner "META-INF" für jedes Java-Archiv entfernen, bevor Sie "SignC2OJars" ausführen.

8. Wenn der Schlüsselspeicher mehr als einen Alias enthält, ändern Sie die Connector-Eingabe in "server.xml". Die Datei "server.xml" befindet sich unter "<Installationsverzeichnis>\server\c2o\deploy\jbossweb-tomcat55.sar\server.xml". Fügen Sie die Zeile in Fettschrift hinzu:

   ```
   <Connector port="${tomcat.secure.port}"
   address="${jboss.bind.address}"
      maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
      emptySessionPath="true"
      scheme="https" secure="true" clientAuth="false"
      keystoreFile="${itpam.web.keystorepath}"
      keyAlias="${itpam.web.keystorealias}"
      keystorePass="${itpam.web.keystore.password}" sslProtocol =
      "${SSL_PROTOCOL}" algorithm = "${X509_ALGORITHM}"
      useBodyEncodingForURI="true"/>
   ```

9. Starten Sie den Koordinationsrechner (siehe Seite 207).

10. Wiederholen Sie diesen Vorgang für jeden Koordinationsrechner, der das neue Zertifikat verwenden soll.

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Verwalten der DNS-Hostnamen

Sie können den Hostnamen für einen Koordinationsrechner ändern. Wenn der Hostname zum Beispiel nicht der unterstützten Syntax entspricht, können Sie ihn aktualisieren. Wenn Sie CA Process Automation mit einem ungültigen DNS-Hostnamen installiert haben, der eingeschränkte Zeichen enthält, wie z. B. Unterstriche, dann erstellen Sie ein Alias, das den DNS-Standards entspricht. Ersetzen Sie dann den ungültigen Hostnamen manuell durch dieses Alias in Ihrer "OasisConfig.properties"-Datei.

Gehen Sie folgendermaßen vor:

1. Erstellen Sie ein Alias. Weitere Informationen finden Sie unter Aktivieren von DNS zur Behebung von ungültigen Hostnamen.
2. Melden Sie sich als ein Administrator am Server an, auf dem der Domänen-Koordinationsrechner installiert ist.
3. Navigieren Sie zum folgenden Ordner, wobei "Installationsverzeichnis" für den Installationspfad des Domänen-Koordinationsrechners steht:

   `*Installationsverzeichnis*/server/c2o/.config`
4. Öffnen Sie die Datei "OasisConfig.properties" mit einem Editor.
5. Verwenden Sie "Suchen", um folgende Eigenschaft zu finden:

   `oasis.local.hostname`
6. Ändern Sie den Wert für die Eigenschaft "oasis.local.hostname=".
7. Speichern Sie die Datei, und schließen Sie den Editor.
8. Starten Sie den Koordinationsrechner-Service neu.
   a. Stoppen Sie den Koordinationsrechner (siehe Seite 206).
   b. Starten Sie den Koordinationsrechner (siehe Seite 207).

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Syntax für DNS-Hostnamen

Es gibt viele Standorte, in denen Sie einen FQDN oder eine IP-Adresse eingeben können. Wenn Ihre DNS-Hostnamen einen Unterstrich enthalten oder in irgendeiner Weise nicht der erforderlichen Syntax entsprechen, geben Sie die IP-Adresse an.

Gültige DNS-Hostnamen:

- Beginnen mit einem alphabetischen Zeichen.
- Enden mit einem alphanumerischen Zeichen.
- Enthalten 2-24 alphanumerische Zeichen.
- Können das Sonderzeichen Minus (-) enthalten.

  Wichtig! Das Minuszeichen (-) ist das einzige Sonderzeichen, dass in DNS-Hostnamen erlaubt ist.

Deaktivieren der Catalyst Process Automation Services

Catalyst Process Automation Services ist standardmäßig aktiviert. Sie können sie deaktivieren, indem Sie einen Eigenschaftswert in der Datei "OasisConfig.properties" ändern.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich als ein Administrator am Server an, auf dem der Domänen-Koordinationsrechner installiert ist.
2. Stoppen Sie den Koordinationsrechner (siehe Seite 206).
3. Wechseln Sie zum folgenden Ordner:

   Installationsverzeichnis/server/c2o/.config
4. Öffnen Sie die Datei "OasisConfig.properties".
5. Scrollen Sie zum UCF-eingebetteten Connector im Abschnitt "jboss-service.xml" der Datei "OasisConfig.properties".
6. Ändern Sie den Wert der Eigenschaft "ucf.connector.enabled" zu "false". Zum Beispiel:

   ```
   ucf.connector.enabled=false
   ```
7. Speichern Sie die Datei, und schließen Sie den Editor.
8. Starten Sie den Koordinationsrechner (siehe Seite 207).

Weitere Informationen:

Oasis-Konfigurationseigenschaftsdatei (siehe Seite 433)

Anhang C: OasisConfig.Properties-Verweis

Dieser Abschnitt enthält das folgende Thema:

Die OasisConfig.properties-Textdatei steuert CA Process Automation. Die beim Installieren des Domänen-Koordinationsrechners vom Installationsprogramm vorgenommene Auswahl sowie die Voraussetzungen und Objekte werden als Parameterwerte in der Datei "OasisConfig.properties" gespeichert.

Wichtig! Beschränken Sie die Aktualisierung der Datei "OasisConfig.properties" auf einen vertrauenswürdigen Administrator.

Dieses Handbuch umfasst die folgenden Themen mit Bezug auf die Aktualisierung der Datei "OasisConfig.properties":

- Steuern von Zwischenspeichern von CA EEM-Aktualisierungen (siehe Seite 80).
- Ändern des SNMP-Traps-Listener-Ports (siehe Seite 348).
- Konfigurieren von Domäneneigenschaften (siehe Seite 156).
- Steuern des Zeitlimits für CA Process Automation (siehe Seite 20).
- Erstellen und Implementieren von eigenen Zertifikaten für CA Process Automation (siehe Seite 422).
- Deaktivieren der Catalyst Process Automation Services (siehe Seite 428).
- Implementieren Ihres Vertrauenswürdigen SSL-Zertifikats eines Drittanbieters für CA Process Automation (siehe Seite 425).
- Verwalten der DNS-Hostnamen (siehe Seite 427).
- Verwalten von IP-Adressen (siehe Seite 413).
- Festlegen der maximalen Anzahl von CA EEM-Anwendern oder -Gruppen (siehe Seite 64).

Das *Installationshandbuch* enthält die folgenden Themen in Bezug auf die Aktualisierung der Datei "OasisConfig.properties":

- Aktivieren der Abmeldung in CA Process Automation für SSO
- Aktivieren der NTLM-Durchleitungs-Authentifizierung nach der Installation
- Generieren von SSL-Zertifikatsdateien
- Verwalten der DNS-Hostnamen
- Voraussetzungen für die Port-Planung
- Lösen eines Port-Konflikts für einen Agenten

Das *Referenzhandbuch für Inhaltsdesign* enthält das folgende Thema mit Bezug auf die Aktualisierung der Datei "OasisConfig.properties":

- Operator-Ports

Das *Webservice-Referenzhandbuch* enthält die folgenden Themen in Bezug auf die Aktualisierung der Datei "OasisConfig.properties":

- Kommunikationen
- executePendingInteraction

Oasis-Konfigurationseigenschaftsdatei

Die Oasis-Konfigurationseigenschaftsdatei (OasisConfig.properties) enthält die Eigenschaftseinstellungen für alle Aspekte von CA Process Automation. Die Datei befindet sich im Ordner "*Installationsverzeichnis*/server/c2o/.config". Alle Anwender mit Zugriff auf den Speicherort der CA Process Automation-Installation können die Dateien ändern. Ziehen Sie in Erwägung, den Zugriff auf diesen Speicherort zu beschränken. Bestimmte Werte dürfen *nicht* bearbeitet werden.

Zu den Einstellungen zählen:

USE_DEPRECATED_COMMS_V1

(Nur für Agenten) Bestimmt während des Starts eines Agenten, ob der neue Kommunikationsmodus oder der veraltete Kommunikationsmodus verwendet wird. Dies ist ein boolescher Wert.

Wenn das Kontrollkästchen "Veraltete Kommunikation verwenden" in den Eigenschaften eines Agenten aktiviert ist, dann wird dieser Wert auf "Wahr" festgelegt. CA Process Automation:

- Beendet die Web-Socket-Verbindung vom Agenten und gibt diese Informationen anschließend vor der Beendigung an alle Koordinationsrechner weiter.
- Bereinigt die Serverzuordnung, wo diese Verbindungsdetails gespeichert sind.

Wenn das Kontrollkästchen "Veraltete Kommunikation verwenden" in den Eigenschaften eines Agenten nicht aktiviert ist, dann wird dieser Wert auf "Falsch" festgelegt.

- Der Agent erstellt eine neue Web-Socket-Verbindung und sendet Verbindungsdetails für den Koordinationsrechner.
- Der Koordinationsrechner speichert diese Verbindungsdetails in einer Serverzuordnung.

Weitere Informationen finden Sie unter "Festlegen des Agent-Kommunikationsmodus (siehe Seite 232)".

DOMAINID

Definiert die eindeutige ID für die Domäne.

Beispiel

`ac04f945-f08b-4308-aa9c-c3fd95964f4d`

CLUSTERNODEID

Bestimmt einen eindeutigen Knoten in einem Cluster.

Beispiel

`8d11558a-3bf7-43d9-b394-4c055229e9ae`

KEYSTOREID

Gibt das Kennwort des Schlüsselspeichers an.

Beispiel

`ac04f945-f08b-4308-aa9c-c3fd95964f4d`

itpam.web.keystorepath

Definiert den Pfad des Schlüsselspeichers, der zum Signieren von JAR-Dateien verwendet wird.

Beispiel

```
C:/Programme/CA/PAMcert_Java7_Node2/server/c2o/.config/c2ok
eystore
```

itpam.web.keystore.password

Definiert das Kennwort des Schlüsselspeichers, der zum Signieren von JAR-Dateien verwendet wird.

Beispiel


```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZLQotQj5
5Y8dPGRRXkrF4yTyk/IwzTcT0rLY+pWeGrGHaRKnlcXHL3fr7pYIzjVhoGd
rnRxSO4Prl70rIxqs3fCGIgFVIAnOzICQ9ct4qXIBIPnxQcgflrF0WDdaIj
CS6ubKwe9Wxhn0xjnmctvkLnMC1L74b48yQd9yhWSMAgpLAPLPJiMz/VoIz
cFVylqLS44KdM+wH6b6xkqVJECSH1GolBG2QUj/2
```


itpam.web.keystorealias

Definiert den Aliasnamen des Zertifikats des Schlüsselspeichers, der zum Signieren von JAR-Dateien verwendet wird.

Beispiel

`ITPAM`

CERTPASSWORD

Definiert das Kennwort, das verwendet wird, um Zugriff auf den Schlüsselspeicher zu steuern, der verwendet wird, um Kennwörter und andere kritische Daten zu verschlüsseln.

Beispiel


```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZXNASLuj
iOdl6POYm8CwjBTHnFUlbXQLcPqd+xc7oJkPF5X3cq8UHbEYL4iH+01b1Em
wHhw9uPXqDABcJqIJ+ECmODDAMn7rytSWqli+oxKp+e5scp1fnHjF1ENCKZ
NasYy6nF6vPozT9qLmB7DhzuFAvg8Av9J/U4ngYrZ5AMdU1sFP5Ddf3nw==
```


oasis.database.username

Definiert den Anwendernamen für den Bibliotheksdatenbankserver.

Beispiel

`sa`

oasis.database.password

Gibt das Kennwort an, das mit dem angegebenen Namen des Bibliotheksdatenbankservers verbunden ist.

Beispiel

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZSSb28pT
xSL4fxuv+8IV8zLz+S6jwleU4mpQTDTM1xmwQ037qmAjDO74Y569W3LIP0v
BUEkJ30raf3/RsodMLdL3L51cnz8Gus4mJfGJla7WdTtzx0ts0BuUFPxZ1p
OpHOUUljFHn73243Iv7/pXIQe+O8lrHB00XotDicrleXavs+8sXSIPqKyX3
gmjy6LUZ
```

oasis.database.dbhostname

Definiert den Hostnamen des Bibliotheksdatenbankservers.

Beispiel

```
lodivsa205
```

oasis.database.dbport

Definiert die Verbindungsportnummer des Bibliotheksdatenbankservers.

Beispiel

```
1433
```

oasis.database.connectionurl

Definiert die JDBC-Verbindungs-URL der Bibliotheksdatenbank.

Beispiel

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.database.databasetype

Definiert den Typ der Bibliotheksdatenbank.

Beispiel

```
MSSQLServer2005
```

oasis.database.dialect

Definiert die anwenderspezifische Dialektklasse der Bibliotheksdatenbank.

Beispiel

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

oasis.database.genericdialect

Definiert die Dialektklasse der Bibliotheksdatenbank.

Beispiel

```
org.hibernate.dialect.SQLServerDialect
```

oasis.database.driver

Definiert den vollqualifizierten Namen der JBDC-Treiberklasse.

Beispiel

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.database.typemapping

Definiert die Typenzuordnung für die Datenquelle.

Beispiel

```
MS SQLSERVER2000
```

oasis.database.exceptionsorter

Definiert eine Klasse, die die Schnittstelle "org.jboss.resource.adapter.jdbc.ExceptionSorter" implementiert. Die Schnittstelle prüft Datenbankausnahmen, um zu bestimmen, ob sie auf einen Verbindungsfehler hinweisen.

Beispiel

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.database.validConnectionChecker

Definiert eine Klasse, die die Schnittstelle "org.jboss.resource.adapter.jdbc.ValidConnectionChecker" implementiert. Die Schnittstelle stellt einen "SQLException isValidConnection(Connection e)"-Modus bereit. Die Anwendung ruft den Modus mit einer Verbindung auf, die vom Pool zurückgegeben wird, um seine Gültigkeit zu testen.

Beispiel

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConn
ectionChecker
```

oasis.database.datasource.class

Definiert die Datenquellenklasse.

Beispiel

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

oasis.database.additionalparamurl

Definiert Parameter, die verwendet werden, um die Datenbankverbindung zu erstellen.

Beispiel

```
responseBuffering=full;SelectMethod=cursor;
```

oasis.database.lib.dbname

Definiert den Namen der Bibliotheksdatenbank.

Beispiel

```
pamgacert_cluster_JDK7_rep
```

oasis.database.queues.dbname

Definiert den Namen der Warteschlangendatenbank.

Beispiel

```
pamgacert_cluster_JDK7_run
```

oasis.reporting.database.databasetype

Definiert den Typ von Berichtsdatenbank.

Beispiel

```
MSSQLServer2005
```

oasis.reporting.database.username

Definiert den Anwendernamen für den Berichtsdatenbankserver.

Beispiel

```
sa
```

oasis.reporting.database.password

Definiert das Kennwort, das mit dem angegebenen Anwender für den Berichtsdatenbankserver verknüpft ist.

Beispiel

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZoIzz9oH
5OU4XRkOaeLblNqEYDsaXNGiMg9LSy2P7gsVLG0ea32nBlUIvXgEXhiKfGz
IbCmYFgYoFg0sVBlnY/k1sAeZ21z20sw5Yr9HC2B3+IRoyy5LXCmByMUMc7
Ywq/BocPnw4e1DBDDfGqCQL/6ciK4CT1C7hU/V3Y4Ktrc9IsPK1aXeNRM1q
vpVwBAtG
```

oasis.reporting.database.dbhostname

Definiert den Hostnamen des Berichtsdatenbankservers.

Beispiel

```
lodivsa205
```

oasis.reporting.database.dbport

Definiert die Verbindungsportnummer des Berichtsdatenbankservers.

Beispiel

```
1433
```

oasis.reporting.database.genericdialect

Definiert die Dialektklasse der Berichtsdatenbank.

Beispiel

```
org.hibernate.dialect.SQLServerDialect
```

oasis.reporting.database.driver

Definiert den vollqualifizierten Namen der JBDC-Treiberklasse.

Beispiel

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.reporting.database.typemapping

Definiert die Typenzuordnung für die Datenquelle.

Beispiel

```
MS SQLSERVER2000
```

oasis.reporting.database.dialect

Definiert die anwenderspezifische Dialektklasse der Berichtsdatenbank.

Beispiel

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.reporting.database.ValidConnectionQuery

Definiert eine SQL-Anweisung, auf einer Verbindung ausgeführt zu werden, bevor sie vom Pool zurückgegeben wird, um seine Gültigkeit zum Testen veralteter Poolverbindungen sicherzustellen. Beispiel: select count(*) from x.

Beispiel

```
select 1
```

oasis.reporting.database.connectionurl

Definiert die JDBC-Verbindungs-URL der Berichtsdatenbank.

Beispiel

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.reporting.database.additionalparamurl

Definiert die zusätzlichen zu verwendenden Parameter für das Erstellen der Datenbankverbindung.

Beispiel

```
;responseBuffering=full;SelectMethod=cursor;
```

FIPS_COMPLIANT

Gibt an, ob der CA Process Automation-Server FIPS-kompatibel ist.

Beispiel

```
true
```

oasis.reporting.database.dbname

Definiert den Namen der Berichtsdatenbank.

Beispiel

```
pamgacert_cluster_JDK7_rpt
```

oasis.runtime.database.dbtype

Definiert den Laufzeitdatenbanktyp.

Beispiel

```
MSSQLServer2005
```

oasis.runtime.database.username

Definiert den Anwendernamen für den Laufzeitdatenbankserver.

Beispiel

```
sa
```

oasis.runtime.database.password

Definiert das Kennwort, das mit dem angegebenen Anwender für den Laufzeitdatenbankserver verknüpft ist.

Beispiel


```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZSOIjQ79
jp66tm5E7ZYxLV2yqtVV54HRVs+xvNksG7p1pzTZOoOXahwS0XOcVoMl8Mz
nkgQgVOllCIU/YBx6lT3ZAxnzOMY2xBQnIp5xTxw0Dv5eqqTvpOnm6P2vPO
S1RzYGA6GRt3VdASiTZwZs/BkIX/sY+6C52V/x5Eg7l4hff6/6gS6wvRHdJ
G/sXU6D6
```


oasis.rntime.database.dbhostname

Definiert den Hostnamen des Laufzeitdatenbankservers.

Beispiel

```
lodivsa205
```

oasis.runtime.database.port

Definiert die Verbindungsportnummer des Laufzeitdatenbankservers.

Beispiel

```
1433
```

oasis.runtime.database.dialect

Definiert die anwenderspezifische Dialektklasse der Laufzeitdatenbank.

Beispiel

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

oasis.runtime.database.genericdialect

Definiert die Dialektklasse der Laufzeitdatenbank.

Beispiel

```
org.hibernate.dialect.SQLServerDialect
```

oasis.runtime.database.driver

Definiert den vollqualifizierten Namen der JBDC-Treiberklasse.

Beispiel

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.runtime.database.typemapping

Definiert die Typenzuordnung für die Datenquelle.

Beispiel

```
MS SQLSERVER2000
```

oasis.runtime.database.exceptionsorter

Definiert eine Klasse, die die Schnittstelle "org.jboss.resource.adapter.jdbc.ExceptionSorter" implementiert, um Datenbankausnahmen zu prüfen und um zu bestimmen, ob die Ausnahme einen Verbindungsfehler anzeigt.

Beispiel

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.runtime.database.ValidConnectionQuery

Definiert eine SQL-Anweisung, auf einer Verbindung ausgeführt zu werden, bevor sie vom Pool zurückgegeben wird, um seine Gültigkeit zum Testen veralteter Poolverbindungen sicherzustellen. Beispiel: select count(*) from x.

Beispiel

```
select 1
```

oasis.runtime.database.validConnectionChecker

Definiert eine Klasse, die die Schnittstelle "org.jboss.resource.adapter.jdbc.ValidConnectionChecker" implementiert, um eine SQLException isValidConnection(Connection e)-Methode bereitzustellen. Eine vom Pool zurückgegebene Verbindung ruft diese Methode auf, um ihre Gültigkeit zu testen.

Beispiel

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConn
ectionChecker
```

oasis.runtime.database.datasource.class

Definiert die Datenquellenklasse.

Beispiel

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

oasis.runtime.properties.table.create.stmt

Definiert die zu verwendende SQL-Anweisung, um die Eigenschaftstabelle zu erstellen, sofern sie nicht vorhanden ist. Diese Anweisung soll vom Anwender nicht geändert werden, da die Anwendung den richtigen Wert für die relevante Datenbank standardmäßig konfiguriert.

Beispiel

```
create table properties (propkey varchar(255) NOT
NULL,propvalue NVARCHAR(MAX),PRIMARY KEY (propkey))
```

oasis.runtime.database.connectionurl

Definiert die JDBC-Verbindungs-URL der Laufzeitdatenbank.

Beispiel

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.runtime.database.additionalparamurl

Definiert die zusätzlichen Parameter, die verwendet werden, um die Datenbankverbindung zu erstellen.

Beispiel

```
;responseBuffering=full;SelectMethod=cursor;
```

oasis.runtime.database.driver.name

Definiert den Treibernamen der Laufzeitdatenbank.

Beispiel

```
com.microsoft.sqlserver.jdbc.SQLServerDriver (für eine
MSSQL-Datenbank)
```

oasis.runtime.database.dbname

Definiert den Namen der Laufzeitdatenbank.

Beispiel

```
pamgacert_cluster_JDK7_run
```

oasis.security.server.type

Definiert den Sicherheitsservertyp, der für die Authentifizierung und Autorisierung verwendet wird.

Beispiel

```
EEM
```

oasis.policy.type

Definiert den Anmeldungsrichtlinientyp.

Beispiel

```
EEM
```

certificatefolderFullpath

Definiert den Pfad des Ordners, der das Sicherheitszertifikat enthält. Der Pfad ist relativ zum c2o-Ordner.

Beispiel

Installationsverzeichnis/server/c2o/.c2orepository/public/certification/

oasis.eem.backend.server.location

Definiert den Hostnamen des Computers, der den EEM-Sicherheitsserver hostet.

Beispiel

```
lodivsa205
```

oasis.eem.application.name

Definiert den Anwendungsnamen auf dem EEM-Server, auf dem die Richtlinien für die aktuelle CA Process Automation-Instanz definiert werden.

Beispiel

`pamgacert_cluster_JDK7`

isFipsMode

Gibt an, ob der EEM-Server im FIPS-Modus ausgeführt wird.

Beispiel

`false`

oasis.eem.certificate.path

Definiert den Namen des Sicherheitszertifikats.

Beispiel

`PAM.p12`

eiamCertKeyPath

Definiert den Namen der Sicherheitszertifikatsschlüsseldatei, die für die Authentifizierung verwendet wird. Diese Eigenschaft ist nur verfügbar, wenn isFipsMode=true vorliegt.

Beispiel

`PAM.key`

oasis.eem.certificate.password

Definiert das Kennwort, das mit dem EEM-Sicherheitszertifikat verbunden ist. Diese Eigenschaft ist nur verfügbar, wenn isFipsMode=false vorliegt.

Beispiel

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZdD65vFT
Vmbn8aaZxjot9QCUIfPEey1H8/KGtNShgrronJk0rMtqliDMrNo2VE+xoAU
DcfmT9IPCQsAe497w1xUBkHg8PbZNjWVkPpFYw496eFiwiq7AoyB8WCoUrx
8wVnkMjoGs1BqDND+kjHcnUt9HLljYgxatT7Q2FpbTA7+Qag0W9gSv2oH4i
BsUjVs22
```

ntlm.enabled

Gibt an, ob die NTLM-Authentifizierung aktiviert ist. Wenn Sie diesen Port ändern, entfernen Sie den .c2o-Ordner, sofern er vorhanden ist, im Ordner ${Installation Dir}/server/c2o/.system.

oasis.jxta.port

Definiert den für Kommunikation mit anderen Koordinationsrechnern oder Agenten zu verwendenden Port.

Beispiel

`7001`

oasis.jxta.host

Definiert den Hostnamen des Computers, der für Kommunikation mit dem Koordinationsrechner oder Agenten verwendet wird.

Beispiel

`*name*03-I40136.ca.com`

oasis.local.hostname

Gibt den Hostnamen des Computers an, auf dem CA Process Automation installiert ist.

Beispiel

`*name*03-I40136.ca.com`

oasis.server.isCluster

Gibt an, ob diese CA Process Automation-Instanz geclustert ist.

Beispiel

`true`

loadbalancer.worker.node

Definiert den Namen dieses Knotens im Cluster. Diese Eigenschaft ist nur verfügbar, wenn sie ein Teil des Clusters ist.

Beispiel

`node2`

oasis.snmptrigger.service.port

Definiert den lauschenden Port für SNMP-Auslöser.

Beispiel

`162`

oasis.transport.secure

Gibt an, ob die Kommunikation sicher ist.

Beispiel

`true`

AcceptAllSSLCertificates

Gibt an, ob alle Zertifikate in der sicheren Kommunikation akzeptiert werden sollen.

Beispiel

`true`

oasis.reject.unnecessary.approval

Gibt an, ob ein nicht für die Genehmigung konfiguriertes Interaktionsformular abgelehnt werden sollte.

Beispiel

`true`

managementconsole.timeout

Definiert die Zeitüberschreitung (in Minuten) für CA Process Automation. Die Zeitüberschreitung ist das Intervall, in dem sich CA Process Automation im Leerlauf befinden kann, nachdem die Sitzung abläuft.

Beispiel

```
30
```

eem.connection.retries

Definiert die Anzahl von Wiederholungen für die Authentifizierung, wenn der Sicherheitsserver EEM ist.

Beispiel

```
3
```

SSL_PROTOCOL

Definiert den SSL-Protokoll-Typ. Ist die IBM Corporation der Java-Anbieter, wird das SSL-Protokoll verwendet. Ansonsten wird TLS verwendet.

Beispiel

```
TLS
```

X509_ALGORITHM

Definiert den Algorithmus, der für SSL-Zertifikate verwendet wird. Ist die IBM Corporation der Java-Anbieter, lautet der verwendete Algorithmus IbmX509. Ansonsten wird SunX509 verwendet.

Beispiel

```
SunX509
```

oasis.publisher.name

Definiert den Namen, unter dem diese CA Process Automation-Instanz lizenziert wird.

Beispiel

```
CA
```

jboss.partition.udpgroup

Definiert die Multicast-Adresse für diesen Clusterknoten.

Beispiel

```
228.1.46.192
```

jboss.rmi.port

Definiert den Port des RMI-Namensgebungsdiensts.

Beispiel

```
1098
```

jboss.jndi.port

Definiert den lauschenden Port für den Bootstrap-JNP-Dienst (JNDI-Anbieter).

Beispiel
`1099`

jboss.rmi.classloader.webservice.port

Definiert den Port, der für den einfachen HTTP-Dienst verwendet wird, der Anforderungen für Klassen, für das dynamische Laden von RMI-Klassen und "org.jboss.web.WebService" unterstützt.

Beispiel
`8083`

jboss.rmi.object.port

Definiert den RMI-Server-Socket-Abhörport, zu dem RMI-Clients eine Verbindung herstellen, wenn sie über eine Proxy-Schnittstelle kommunizieren.

Beispiel
`4444`

jboss.pooledinvoker.serverbind.port

Definiert den in einem Pool zusammengefassten Port der aufrufenden Serverbindung.

Beispiel
`4445`

remoting.transport.connector.port

Definiert den Port der Remote-Serverbindung.

Beispiel
`4448`

jboss.ha.jndi.port

Definiert den Port, auf dem der HA-JNDI-Stub verfügbar gemacht wird.

Beispiel
`1100`

jboss.ha.jndi.rmi.port

Definiert den RMI-Port, den der HA-JNDI-Service verwendet, wenn eine Verbindung besteht.

Beispiel
`1101`

jboss.ha.rmi.object.port

Definiert den RMI-Objektport, den JRMPInvokerHA verwendet.

Beispiel
`4447`

jboss.ha.pooledinvoker.serverbind.port

Definiert den in einem Pool zusammengefassten Port der aufrufenden HA-Serverbindung.

Beispiel

`4446`

jboss.mcast.jndi.autodiscovery.port

Definiert den Multicast-Gruppenport, der für die JNDI-AutoErmittlung verwendet wird. Dieser Port wird in "cluster-service.xml" und "hajndi-jms-ds.xml in deploy/jms" definiert.

Beispiel

`1102`

jboss.mcast.ha.partition.port

Definiert den Multicast-UDP-Port für HAPartition. Dieser Port wird in "cluster-service.xml" und "jmx-console.war/WEB-INF/web.xml" definiert.

Beispiel

`45566`

jboss.mcast.http.sessionreplication.port

Definiert den Multicast-UDP-Port für die HttpSession-Replikation. Dieser Port wird in "tc5-cluster-service.xml" definiert.

Beispiel

`45567`

tomcat.connector.http.port

Definiert den Port für die Connector-Komponente, die das HTTP/1.1-Protokoll unterstützt. Durch diese Eigenschaft kann Catalina als ein eigenständiger Webserver fungieren, und zwar zusätzlich zu seiner Fähigkeit, Servlets und JSP-Seiten auszuführen. Der Port wird auch in "jboss-ws4ee.sar/META-INF/jboss-service.xml for Axis SService" konfiguriert.

Beispiel

`8080`

tomcat.connector.ajp.port

Definiert den Port für die Connector-Komponente, die mit einem Webconnector über das AJP-Protokoll kommuniziert.

Beispiel

`8009`

tomcat.secure.port

Definiert den sicheren Port, den der SSL-Connector verwendet. Dieser Port wird nicht verwendet. Dieser Port ist der gleiche Port, der wie folgt konfiguriert wird:

- redirectPort für den AJP-Connector in server.xml
- WebServiceSecurePort für Axis Service in jboss-ws4ee.sar/META-INF/jboss-service.xml

Der Port wird nur verwendet, wenn der SSL-Connector aktiviert ist.

Beispiel

```
8443
```

jboss.uil.serverbind.port

Definiert den Port, mit dem Unified Invocation Layer-Service-Clients (UIL) eine Verbindung herstellen, wenn sie eine Verbindung mit dem JBossMQ-Server herstellen.

Beispiel

```
8093
```

oasis.protection.level

Gibt die CA Process Automation-Schutzebene an. Im sicheren Modus wird die Schutzebene auf CONFIDENTIAL festgelegt, ansonsten ist sie auf NONE festgelegt.

Werte: NONE, INTEGRAL oder CONFIDENTIAL.

itpam.initialperiodicheartbeatfrequency

Definiert die anfängliche Heartbeat-Frequenz (in Minuten).

Beispiel

```
2
```

system.encoding

Definiert die Verschlüsselung dieses Systems.

Beispiel

```
Cp1252
```

eem.max.search.size

Definiert die Höchstanzahl von Datensätzen, um gleichzeitig in EEM zu suchen.

Beispiel

```
10000
```

jboss.remoting.transport.Connector.port

Definiert einen JBoss-bezogenen Port.

Beispiel

```
3873
```

OAPort

Definiert einen JBoss-bezogenen Port.

Beispiel
```
3528
```

OASSLPort

Definiert einen JBoss-bezogenen Port.

Beispiel
```
3529
```

scripts.tmpDir

Definiert den Wert des temporären Verzeichnisses, das Skripts ausführt.

Beispiel:
```
C:/Users/ADMINI~1/AppData/Local/Temp/2
```

oasis.powershell.setexecutionpolicy

Gibt an, ob der Anwender eine Option zum Ändern der PowerShell-Ausführungsrichtlinie während der Installation ausgewählt hat.

Beispiel
```
false
```

oasis.powershell.path

Definiert den PowerShell-Pfad auf dem Hostcomputer.

Beispiel
```
C:/Windows/System32/WindowsPowerShell/v1.0
```

override.jvm.tmpdir

Gibt an, ob die Systemvariable java.io.tmpdir überschrieben werden soll. Mit dem Standardwert (true) kann der Server die Systemvariable zu c2oHome/tmp referenzieren. Legen Sie diese Eigenschaft auf false fest, wenn der Server die Systemvariable nicht zu c2oHome/tmp referenzieren soll.

Beispiel
```
true
```

jboss.default.jgroups.stack

Definiert den standardmäßigen Stapeltyp, der von JGroups für die Verwendung festgelegt wird, damit die Anwendung weiterhin ausgeführt wird.

Beispiel
```
tcp
```

jboss.jgroups.tcp.tcp_port

Definiert den TCP-Port für TCP-basiertes Clustering in JBoss.

Beispiel
```
7600
```

jboss.jgroups.tcp_sync.tcp_port

Definiert den TCP-Synchronisationsport für TCP-basiertes Clustering in JBoss.

Beispiel

`7650`

jboss.messaging.datachanneltcpport

Definiert den TCP-basierten Messaging-Datachannel-Port.

Beispiel

`7900`

jboss.messaging.controlchanneltcpport

Definiert den TCP-basierten Messaging-Control-Channel-Port.

Beispiel

`7901`

jts.default.tx.reaper.timeout

Definiert eine nichtnegative Ganzzahl, die der JBossTS benötigt.

Beispiel

`120000`

jboss.transaction.timeout

Definiert die Zeit, wann der Reaper nach einer Zeitüberschreitung eine Zeitüberschreitung für fortlaufenden Transaktionen beginnt. Der JBoss erfordert diese Eigenschaft.

Beispiel

`300`

jboss.service.binding.port

Definiert die Datei "Ref deploy/messaging/remoting-bisocket-service.xml". JBoss Messaging erfordert diese Eigenschaft.

Beispiel

`4457`

jboss.remoting.port

Definiert die Datei "Ref deploy/jmx-remoting.sar". JBoss Remoting erfordert diese Eigenschaft.

Beispiel

`1090`

jboss.jbm2.port

Definiert den Kommunikationstransport zu JBoss Messaging. JBoss Messaging 2 Netty erfordert diese Eigenschaft.

Beispiel

`5445`

jboss.hbm2.netty.ssl.port

Die JBoss. SSL-Version von Netty erfordert diese Eigenschaft.

Beispiel

`5446`

jboss.tx.recovery.manager.port

Definiert die Datei "Ref deploy/transaction-jboss-beans.xml". Der JBossTS Recovery Manager erfordert diese Eigenschaft.

Beispiel

`4712`

jboss.tx.status.manager

Definiert die Datei "Ref deploy/transaction-jboss-beans.xml". Der JBossTS Transaction Status Manager erfordert diese Eigenschaft.

Beispiel

`4713`

jboss.tx.manager.sock.pid.port

Definiert die Datei "Ref deploy/transaction-jboss-beans.xml". Der JBossTS erfordert diese Eigenschaft.

Beispiel

`4714`

ucf.payload.file

Definiert den Namen der Datei, die die Catalyst-Container-Nutzdaten enthält.

Beispiel

`catalyst.installer.payload.zip`

catalyst.container.name

Definiert den Namen des Catalyst-Containers.

Beispiel

`node0`

ucf.connector.enabled

Gibt an, ob Catalyst Process Automation Services aktiviert ist.

Beispiel

`false`

ucf.payload.override

Gibt an, ob die Nutzdaten überschrieben werden sollen (wenn die Nutzdaten vorhanden sind).

Beispiel

`false`

ucf.pax.web.http.port

Definiert den /container/etc/org.ops4j.pax.web.cfg-Port.

Beispiel
`8181`

ucf.bus.hostname

Definiert den Catalyst-Bus-Hostnamen in registry/topology/physical/node0/catalyst-bus/bus.properties.

Beispiel
`localhost`

ucf.bus.port

Definiert den Catalyst-Bus-Port in /registry/topology/physical/node0/catalyst-bus/bus.properties.

Beispiel
`61616`

ucf.bus.http.port

Definiert den Catalyst-Bus-HTTP-Port in /registry/topology/physical/node0/catalyst-bus/bus.properties.

Beispiel
`61617`

ucf.max.archive.query.results

Definiert die größtmöglichen Archivabfrageergebnisse.

Beispiel
`30`

use.catalyst.claims.credentials

Gibt an, ob die Catalyst-Ansprüche für die Anmeldeinformationen verwenden werden sollen.

Beispiel
`false`

org.apache.commons.logging.Log

Definiert eine Factory-Klasse für die Instanziierung von Protokollierungen für die Commons Logging.

Beispiel
`org.apache.commons.logging.impl.Log4JLogger`

org.apache.commons.logging.LogFactory

Definiert eine Factory-Klasse für die Instanziierung von Protokollierungen für die Commons Logging.

Beispiel

```
org.apache.commons.logging.impl.Log4jFactory
```

eem.cache.timeout

Dieser vom Anwender hinzugefügte Parameter definiert das maximale Alter des Zwischenspeichers (in Sekunden), während dessen Anwender-Anmeldeinformationen mit den zugeordneten Berechtigungen im Speicher aufbewahrt werden. Wenn dieser Wert auf Null gesetzt wird, wird der CA Process Automation-Autorisierungszwischenspeicher ausgeschaltet, und CA Process Automation sendet jedes Mal, wenn Anwenderberechtigungen benötigt werden, eine Anfrage an CA EEM. Wenn dieser Parameter fehlt, verwendet CA Process Automation 30 Sekunden als Aktualisierungsrate für den sekundären Zwischenspeicher.

Hinweis: Details über die beiden CA EEM-Zwischenspeicher finden Sie unter Steuern der Aktualisierungsrate von Zwischenspeichern mit CA EEM-Aktualisierungen (siehe Seite 80).

Beispiel

30

mail.attachment.buffer.size

Ermöglicht es Ihnen, eine E-Mail mit einer spezifischen Puffergröße herunterzuladen.

Die Maßeinheit ist K. Eine Eingabe von 256 wird von CA Process Automation als 256 K definiert.

Beispiel

mail.attachment.buffer.size=256

mail.imap.fetchsize

Diese Eigenschaft gilt spezifisch für das IMAP-Protokoll und wird für CA Process Automation nicht eingeführt. Diese Eigenschaft ermöglicht es Ihnen, große E-Mail-Anhänge schneller herunterzuladen.

Geben Sie diese Eigenschaft in Byte an.

Beispiel

Um 800 K anzugeben, multiplizieren Sie 800 x 1024.

mail.imap.fetchsize=819200